Departamento de Informática

PROYECTO FIN DE CARRERA

Ingeniería Técnica en Informática de Gestión

ENTORNOS COLABORATIVOS:

SEGURIDAD EN REDES SOCIALES

AUTOR: Víctor Manuel Pérez García

TUTORA: Pilar Aránzazu Herráez López

Leganés, a 18 de Junio de 2012

Título: ENTORNOS COLABORATIVOS: Seguridad en Redes Sociales

Autor: Víctor Manuel Pérez García

Director: Pilar Aránzazu Herráez López

EL TRIBUNAL

Presidente: D. Luis García Sánchez.

Vocal: D. Miguel Ángel Ramos.

Secretaria: Doña Fuensanta Medina.

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 18 de Junio de 2012 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Agradezco todos estos años a mi familia y especialmente a mi madre que lo ha dado todo por mí, sin su enorme apoyo y cariño no lo habría conseguido jamás, además de heredar su vitalidad y energía. A mi mujer Sandra por quererme tanto, entender mi fuerte carácter y multitud de cosas más. Y por último a mis amigos que han estado siempre en los buenos y especialmente en los malos momentos que es donde se demuestra que son verdaderos.

Resumen

Palabras clave:

- *Entornos Colaborativos*
- *Internet*
- *Legislación*
- *Medio Social*
- *Red Social*
- *Seguridad Informática*

Resumen del proyecto:

Este proyecto fin de carrera analiza las amenazas y vulnerabilidades que atentan contra la seguridad informática en el uso de las Redes Sociales. El principal fin de estas amenazas es la de atentar contra la privacidad de los usuarios, lo que deriva directamente en la violación de derechos jurídicos como el Real Decreto 1720/2007 de protección de datos de carácter personal.

Se trata por tanto de un proyecto con una gran investigación y cuyo carácter funcional y de consultoría intenta establecer pautas de conducta y mecanismos de defensa, tanto a las propias empresas proveedoras de las Redes Sociales como a sus usuarios. Usuarios en los que se ha hecho una mención especial a personas que presentan algún tipo de discapacidad psíquica y/o física y a los menores de edad, debido a que son en parte el colectivo más vulnerable.

Abstract

Keywords

- *Collaborative Environments*
- *Internet*
- *Legislation*
- *Social Media*
- *Social Network*
- *Information Security*

Summary of the project

This Final Career Project analizes the threats and vulnerabilities which attempts against informatic security by using Social Networks. This threat main goal is attempting aganist users privacy, what leads a legal rigths violation directly, like royal decree 1720/2007 of personal data protection.

Therefore, it is a proyect with a great investigation whose functional and query features try to stablished beheavior guidelines and defense mechanisms in both, the supplier social network enterprises and users. About users with a special mention to people with mental and/or physical disabilities and minors, because they are the most vulnerable group.

Índice general

Índice de figuras

CAPÍTULO 1

INTRODUCCIÓN

1. INTRODUCCION

En este capítulo se incluye una descripción detallada de lo que es una Red Social y la importancia que están teniendo actualmente en la sociedad gracias a los servicios que proporciona a sus usuarios sin estar exentos de riesgos y vulnerabilidades.

1.1 Introducción

En primer lugar conviene definir el concepto de ó Redô el cual hace referencia a un conjunto de entidades o nodos (objetos, personas, etc.) conectadas entre sí a través de grafos. Por lo tanto, una red permite que circulen elementos materiales o inmateriales entre estas entidades, según reglas bien definidas.

Figura 0. Representa una Red Social con sus nodos (personas) y sus grafos (líneas de color marrón que conectan a uno o varios nodos) [REF_FIG0].

Según el tipo de entidad involucrada, el término utilizado variará, así existen Redes de Transportes, Redes Telefónicas, Redes neuronales, Redes criminales, Redes Sociales *online*, etc.

Este proyecto se enfoca en las Redes Sociales *online* y una de las definiciones que mejor las describen es que son estructuras sociales que se pueden representar en forma de uno o varios grafos en el cual los nodos representan individuos (a veces denominados actores) y las aristas relaciones entre ellos.

Los fines de una Red Social son muy variados. Van desde encontrar a los compañeros de colegio, instituto y universidad, a amistades de la infancia o a familiares de los que se desconocía su existencia o que por encontrarse tan lejos no se mantiene una relación continua.

También fomentan las relaciones de trabajo y las oportunidades de negocio existentes. Como además estamos hablando de la implantación de las redes a nivel mundial, se pueden ampliar hasta extremos inimaginables las conexiones y los contactos [00].

El modelo de crecimiento de estas plataformas se basa fundamentalmente en un ópproceso viralô, en el que un número inicial de participantes, mediante el envío de invitaciones a través de correos a sus conocidos, ofrece la posibilidad de unirse al portal de la Red Social.

Estos nuevos servicios se configuran como poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como grupos segmentados: ocio, comunicación, profesionalización, etc. Es por ello que están teniendo una gran acogida en todo el mundo.

Desde 1995 las cifras de usuarios de las redes sociales en *Internet* no para de crecer. El número total de usuarios de Redes Sociales en todo el mundo se estima actualmente en más de 940 millones, por lo que el uso de las mismas está tomando una relevancia sin precedentes en el mundo de *Internet* [01].

El 75% de los internautas en España usan redes sociales. España es el 5º país del mundo que más utiliza estas redes superando a Francia y Alemania [02].

Según los últimos datos facilitados por *Facebook*, esta red social ha superado los 800 millones de usuarios en el mundo, entre los cuales 15 millones están en España. Además, la segunda página más vista en España es *Facebook* después de *Google* [02].

Por su parte *Twitter* supera los 200 millones de usuarios en el mundo, de los cuales 100 millones son activos. Aunque *Twitter* no ha facilitado datos oficiales, se estima que esta red puede haber llegado a los 4,5 millones de usuarios en España [02].

Tuenti se caracteriza por aglutinar al público más joven, el 90% de sus usuarios tiene entre 14 y 35 años, y alcanza, en octubre de 2011, los 12 millones de usuarios [02].

La nueva red social de *Google* ha alcanzado recientemente los 62 millones de usuarios en el mundo. Desde su nacimiento, en fase beta en abril de 2011, *Google plus* ha tenido un vertiginoso progreso en cuanto a número de usuarios, aunque aún somos muchos los escépticos que creemos que *Google plus*

no está en posición ni de desbancar a *Facebook*, ni de conseguir la posición de segunda red social con más usuarios. Sobre todo el escepticismo deriva de los datos de usuarios activos, si bien es cierto que *Google plus* tiene 62 millones de usuarios inscritos, sólo un 14% son activos, unos 9 millones [02]

Por su parte *LinkedIn*, la Red Social de profesionales, supera los 135 millones de usuarios en el mundo, llegando en España a los 2 millones [02].

Figura 1. Usuarios de las principales Redes Sociales en España y en el mundo [REF_FIG1].

El perfil del usuario de estas redes es el de una persona de entre 16 y 30 años, de clase alta, que vive en grandes núcleos urbanos y que quiere mantener el contacto con amigos, sólo por diversión, y hablar con parte de la familia que no ven con frecuencia [02].

La importancia de las Redes Sociales *online* no queda exenta de riesgos y ataques malintencionados. Es una preocupación de las organizaciones nacionales, europeas e internacionales (principalmente de la Comisión Europea y del Grupo de trabajo del artículo 29) con competencias en las materias afectadas por el uso de estas redes, que han impulsado la elaboración de normas y recomendaciones. Estas recomendaciones se plasmaron del 15 al 17 de octubre de 2008 en la que se celebró la 30 Conferencia Internacional de Autoridades de Protección de Datos y privacidad en Estrasburgo. En ella se acordó

llevar a cabo una propuesta de regulación normativa de este tipo de plataformas que cumpla con los siguientes requisitos: ser una normativa mundial, legalmente exigible a cualquier tipo de prestador, con independencia de dónde se encuentre ubicado; que dote a los usuarios de una serie de protecciones consideradas básicas a la hora de desarrollar su actividad en la Red; que garantice una protección mínima y básica para los menores, usuarios nativos de este tipo de servicios y especialmente desprotegidos ante éstos, así como que los prestadores establezcan una serie de medidas tecnológicas encaminadas a la protección de los usuarios. De esta forma el pasado mes de noviembre del año 2011 se celebró en México, la 33 Conferencia Internacional de Protección de Datos, en la que se exploró el camino hacia la construcción de las relaciones y las herramientas necesarias para proteger los datos de las personas, independientemente de la cultura, las fronteras nacionales, o los retos derivados de los usos innovadores de la información [03].

1.2. Objetivos

El principal objetivo del proyecto es analizar las cuestiones legislativas y de seguridad informática en las Redes Sociales, y desarrollar propuestas y recomendaciones a tener en cuenta por parte de los proveedores de las Redes Sociales y usuarios de las mismas para poder proteger sus derechos jurídicos y posibles ataques informáticos en el uso de las mismas.

Como objetivos secundarios, se analizan las principales ventajas e inconvenientes que suponen las Redes Sociales debido al gran auge que están experimentando en la actualidad en todo el mundo.

1.3. Fases de desarrollo

En el desarrollo de este proyecto se han pasado por diversas fases, las cuales son explicadas a continuación:

- **Identificar documentación:** En esta fase se ha identificado toda la información necesaria para poder desarrollar con claridad todos los conceptos tratados en este proyecto.

- **Evaluación del proyecto:** En esta fase se realiza una evaluación de todo el proyecto una vez este ha sido finalizado y en la cual se observa si el proyecto cumple con sus objetivos.

1.4. Medios empleados

En la elaboración de este proyecto ha sido de vital importancia la innumerable documentación hallada en *Internet* y los artículos de la Constitución Española, así como la aportación subjetiva del autor en algunos apartados del proyecto.

1.5. Estructura de la memoria

En este apartado se describe cómo está estructurado el presente documento, explicando brevemente el contenido de cada capítulo:

- **Capítulo 1: Introducción**

  En este capítulo se desarrolla todos los conceptos teóricos sobre las Redes Sociales.

- **Capítulo 2: Estado del Arte**

  En este capítulo se hace un repaso de la historia en *internet* y con ello del surgimiento de las primeras Redes Sociales. Se mostrarán todas las ventajas, inconvenientes, tipologías y el vertiginoso crecimiento y desarrollo que han experimentado desde su creación, dando una perspectiva futura de las mismas.

- **Capítulo 3: Seguridad en las Redes Sociales**

  En este capítulo se hace un seguimiento sobre los principales ataques y vulnerabilidades que pueden sufrir las Redes Sociales enfocados principalmente a violar privacidad de los usuarios de las mismas y las defensas a nivel técnico y de usuario para protegerse de dichas amenazas.

- **Capítulo 4: Aspectos jurídicos**

  En este capítulo se hace un repaso sobre todos los derechos jurídicos que atañen a los usuarios de las Redes Sociales.

- **Capítulo 5: Conclusiones y futuras líneas de investigación**

  En este capítulo se presentan las conclusiones del PFC presentado, las principales aportaciones realizadas y algunas de las futuras líneas de trabajo vinculadas a dicho PFC.

- **Capítulo 6: Presupuesto**

  En este apartado se incluye el presupuesto del proyecto con el correspondiente desglose de costes de personal, costes del material y costes totales y la planificación del mismo a través del diagrama de Gantt.

- **Capítulo 7: Glosario**

  En este capítulo se definen y comentan ciertos términos utilizados en el PFC, con el fin de ayudar al lector a comprender mejor los significados de algunas palabras.

- **Capítulo 8: Referencias**

  En este capítulo se definen todas las referencias bibliográficas de documentación encontrada en *Internet.*

CAPÍTULO 2

ESTADO DEL ARTE

2. ESTADO DEL ARTE

2.1. Fundamentos teóricos

Cuando se habla de Redes Sociales, se hace referencia a las plataformas *online* desde las que los usuarios registrados pueden interactuar mediante mensajería sincronía y asíncrona, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediatamente por todos los usuarios de su entorno cooperativo.

El análisis de las Redes Sociales ha irrumpido en muchas ciencias sociales en los últimos veinte años como una nueva herramienta de análisis de los individuos y de sus relaciones sociales. Al centrarse en las relaciones de los individuos (o grupos de individuos) y no en las características de los mismos (raza, edad, ingresos, educación) se han utilizado para el estudio de hábitos, gustos y formas de relacionarse de los grupos sociales.

Cualquier Red Social en *Internet* se fundamenta en la llamada ôTeoría de los seis grados de separaciónô Básicamente dicha teoría significa que si tomamos dos personas diferentes del mundo y tratamos de ver si conocen gente en común llegaremos a la conclusión de que están conectadas por una cadena de personas conocidas que tiene, como máximo, cuatro intermediarios y un total de seis nodos. De esta manera, la red de conocidos de una persona podría extenderse a través de las redes de conocidos de sus conocidos y ser, virtualmente, conocido de toda la humanidad.

Internet y el desarrollo de potentes aplicaciones informáticas que generan plataformas de intercambio de información e interacción entre individuos ha supuesto una auténtica revolución para la aparición del concepto de Red Social tal y como se conoce hoy en día. La universalidad que ofrece la Red permite ampliar el número de contactos y estrechar lazos de unión entre aquellos usuarios que tienen intereses comunes.

2.2. Definición

El concepto de Red Social ha sido ampliamente analizado por profesionales de diferentes sectores, no existiendo en la actualidad un concepto absolutamente cerrado y aceptado por todos ellos.

Una de las definiciones más extendidas de lo que significa una ó Red Socialô la define como una estructura social en la que se realiza un intercambio entre sus miembros, y de los miembros de una red con los de otra, que puede ser otro grupo u otra organización. Esta comunicación dinámica permite sacar un mejor provecho de los recursos que poseen los miembros de estas redes. Los individuos o miembros son llamados ó actoresô o ó nodosô en las publicaciones que detallan el funcionamiento de las Redes Sociales, y se llama ñaristasò a las relaciones entre ellos. Las relaciones entre los miembros de las Redes Sociales pueden girar en torno a un sin número de situaciones tales como el intercambio de información, el financiero, o simplemente la amistad o las relaciones amorosas.

Pero hay una teoría algo más profunda detrás de las Redes Sociales que sostiene que las personas del planeta están relacionadas entre sí a través de no más de seis personas y por eso se la conoce también col el nombre de ó Teoría de los seis grados de separaciónô explicada en el anterior apartado [00].

Existe una teoría de corte similar que es la ó Teoría de los 10 saltosô, basada en que se puede conectar a una persona con las demás en el planeta en solamente 10 saltos: una persona conoce unas 100 personas, y cada uno de ellos se relaciona, en promedio, con otras 100. Así, si la primera persona pide a sus amigos que pasen un mensaje a sus conocidos, casi inmediatamente la primera persona posee una red de 100 x 100 = 10000 conocidos a quienes podría estar pasando la información y entonces podría compartir cosas con ellos en *Internet* y fuera de ella. Así, cada nivel de individuos amplía la cantidad de conocidos del nivel anterior de manera geométrica [04].

Otros conceptos característicos que describen de lo que es una ó Red Socialô

- Formas de interacción social, que se definen fundamentalmente por los intercambios dinámicos entre los sujetos que las forman. Las redes son sistemas abiertos y horizontales y aglutinan a conjuntos de personas que se identifican con las mismas necesidades y posibles problemáticas. Las redes, por tanto, se erigen como una forma de organización social que permite a un grupo de personas potenciar sus recursos y contribuir a la resolución de problemas [05].
- En términos generales, el concepto de red se utiliza para hacer referencia a dos fenómenos: por un lado, se consideran redes todos los conjuntos de interacciones que se dan de forma espontánea, y por el otro, y este es el aspecto que interesa destacar, las redes pretenden organizar esas interacciones espontáneas con un cierto grado de formalidad, en el sentido de establecer intereses, problemáticas, preguntas y fines comunes [05].

2.3. Historia

2.3.1. Historia de *internet*

En **1958** se organiza en EE.UU. la agencia gubernamental de investigación, ARPA (Advanced *Research Projects Agency*) creada en respuesta a los desafíos tecnológicos y militares de Rusia, durante la Guerra Fría, de la cual surgieron una década más tarde los fundamentos de la futura red global de computadores *Internet*. Es la respuesta al lanzamiento realizado un año antes por Rusia del primer satélite artificial, el *Sputnik I*, el suceso, de fuertes implicancias estratégicas y militares ha impactado a los EE.UU.

En **1961** *Leonard Kleinrock* publica desde el MIT (*Massachusetts Institute of Technology*) su primer trabajo sobre la teoría de ó Conmutación de paquetesô que es el envío de datos en una red de computadoras. Un paquete es un grupo de información que consta de dos partes: los datos propiamente dichos y la información de control, en la que está especificado la ruta a seguir a lo largo de la red hasta el destino del paquete. Mil octetos es el límite de longitud superior de los paquetes, y si la longitud es mayor el mensaje se fragmenta en otros paquetes. Se plantea la factibilidad teórica de utilizar esta revolucionaria técnica en lugar de circuitos.

En **1962** un investigador del gobierno de los EE.UU., *Paul Baran*, presenta un proyecto al Departamento de Defensa de EE.UU. de un sistema de comunicaciones mediante computadoras conectadas en una red descentralizada que resultara inmune a ataques convencionales.

En **1965** el investigador del MIT *Lawrence G. Roberts* conectó un ordenador TX2 en *Massachusetts* con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de ordenadores de área amplia jamás construida.

En **1966** los científicos experimentan el uso de fibra óptica como soporte de transmisión de señales telefónicas. *Bob Taylor* en ARPA recibe un subsidio para experimentar un sistema de interconexión mediante ordenadores entre agencias federales y universidades Tres años más tarde concretará esta iniciativa en lo que se conocerá como ARPANET.

En **1969** *Michel Elie*, quien se convertirá en uno de los pioneros de *Internet* ingresa en la UCLA (*University of California*, Los Ángeles), en donde se instala ese mismo año el primer nodo de ARPA, con una beca de investigación del IRIA (Instituto de investigación en informática y automática). Hacia finales

de ese año se establece un enlace entre la computadora de la UCLA y otra del *Stanford Research Institute*. Al mes siguiente, son cuatro las universidades interconectadas.

En **1970** ARPANET había crecido hasta 15 nodos con 23 ordenadores *hosts* (centrales). Un año más tarde *Ray Tomlinson*, escribe el *software* básico de envío-recepción de mensajes de correo electrónico, impulsado por la necesidad que tenían los desarrolladores de ARPANET de un mecanismo sencillo de coordinación. Poco más tarde amplía su valor añadido con un primer programa de correo electrónico para relacionar, leer selectivamente, almacenar, reenviar y responder a mensajes.

También en **1970** el *Network Working Group* (NWG) liderado por *S.Crocker* acabó el protocolo *host* a *host* inicial para ARPANET, llamado *Network Control Protocol* (NCP, protocolo de control de red)

En **1972** ARPA cambia su denominación y es conocida como DARPA (*Defense Advanced Research Projects Agency*) y se realiza la primera demostración pública de la nueva tecnología de ARPANET, las primeras conexiones internacionales se realizan un año más tarde entre el *University College of London* en Inglaterra y *the Royal Radar Establishment* en Noruega.

En **1974** dos investigadores, *Vint Cerf (Stanford University)* y *Robert Kahn*, redactan un memoranda titulado *"A Protocol for Packet Nertwork Internetworking"*, donde explicaban cómo podría resolverse el problema de comunicación entre los diferentes tipos de computadoras.

En **1975** ARPANET es transferida por DARPA al dominio de la Agencia de Comunicaciones para la Defensa de los EE.UU. como una red operacional. DARPA ha estado involucrada desde hace casi dos décadas con el desarrollo tecnológico bajo cuyo orbita se ha desarrollado *Internet*.

En **1976** se establece el protocolo conocido como X-25 para la transmisión de paquetes conmutados en redes públicas. Este mismo año *Vint Cerf* y *Bob Kahn* entre otros demuestran la factibilidad del primer sistema de enlace por radio mediante paquetes conmutados y ARPANET.

En **1978** DARPA formaliza contratos para actualizar el protocolo TCP/IP Este fue el principio de un largo período de experimentación y desarrollo de la tecnología de *Internet*. Partiendo de las tres primeras redes ARPANET, radio y satélite y de sus comunidades de investigación iniciales, el entorno experimental creció hasta incorporar cualquier forma de red.

El crecimiento de ARPANET hizo necesario algunos órganos de gestión: el *Internet Configuration Control Board* fue formado por ARPA en 1979. Más tarde se transformó en el *Internet Activities Board* y luego en el *Internet Architecture Board of the Internet Society.*

En **1980** el Ejército norteamericano adopta como un estándar el protocolo TCP/IP, lo cual permite empezar a compartir la tecnología DARPA basada en *Internet* y llevar a la separación final entre las comunidades militares y no militares.

En **1981**, en un acuerdo sin precedentes entre CSNET y NSF, y DARPA, permite que el tráfico de CSNET compartiera la infraestructura de ARPANET en consecuencia, y de forma similar, la NFS promociona sus redes regionales de NSFNET, inicialmente académicas, para buscar clientes comerciales, expandiendo sus servicios y explotando las economías de escala resultantes para reducir los costes de suscripción para todos, para finales de ese año hay 213 máquinas conectadas. Ese mismo año la corporación IBM presenta sus primeros computadores personales a un precio de 4.500 dólares con una sorprendente repercusión logrando vender más de 65.000 unidades tan solo en los primeros cuatro meses.

- Durante este mismo año *Ted Nelson* esboza su proyecto *Xanadu*, un sistema global de recolección y distribución de toda la documentación escrita mundial en hipertexto, el crecimiento desmesurado de la información durante la próxima década lo convertirá en una utopía.
- *Ira Fuchs* y *Greydon Freeman* crean el servicio BITNET, uniendo a los ordenadores centrales del mundo académico siguiendo el paradigma de correo electrónico como "postales". Con la excepción de BITNET y USENET, todas las primeras redes (como ARPANET) se construyeron para un propósito determinado. Es decir, estaban dedicadas (y restringidas) a comunidades cerradas de estudiosos; de ahí las escasas presiones por hacer estas redes compatibles y, en consecuencia, el hecho de que durante mucho tiempo no lo fueran.

En Francia durante **1983** irrumpe un revolucionario sistema de videotexto ofrecido a través del sistema telefónico de *France Telecom* mediante pequeñas terminales hogareñas para acceder a información de directorios públicos y comunicaciones interpersonales.

Entretanto en **1983** comienza a ser realidad *Internet* cuando la red militar de ARPANET es separada de la dedicada a usos civiles, hasta entonces era usada por un número significativo de organizaciones operativas y de investigación y desarrollo en el área de la defensa. La transición desde NCP a TCP/IP en ARPANET permitió la división en una MILNET para dar soporte a requisitos operativos y una ARPANET para las necesidades de investigación.

En Europa se crea la *"European Unix Network"* (EUNET), conectado a ARPANET, para proporcionar servicios de correo electrónico y servicios *Usenet* a diversas organizaciones usuarias en los Países Bajos, Dinamarca, Suecia e Inglaterra.

En **1986** la *National Science Foundation* (NSF) de EE.UU. inició el desarrollo de NSFNET que se diseñó originalmente para conectar cinco superordenadores. Su interconexión con *Internet* requería unas líneas de muy alta velocidad. Esto aceleró el desarrollo tecnológico de *internet* y brindó a los usuarios mejores infraestructuras de telecomunicaciones. Otras agencias de la Administración norteamericana entraron en *Internet*, con sus inmensos recursos informáticos y de comunicaciones: NASA y el Departamento de Energía (*BACKBONES* de alta velocidad).

Originalmente había un sencillo algoritmo de enrutamiento que estaba implementado uniformemente en todos los *routers* de *Internet*. A medida que el número de redes en *Internet* se multiplicaba, el diseño inicial no era ya capaz de expandirse, por lo que fue sustituido por un modelo jerárquico de enrutamiento con un protocolo IGP (Interior *Gateway Protocol*, protocolo interno de pasarela) usado dentro de cada región de *Internet* y un protocolo EGP (Exterior *Gateway Protocol*, protocolo externo de pasarela) usado para mantener unidas las regiones. Los algoritmos de enrutamiento no eran los únicos en poner en dificultades la capacidad de los routers, también lo hacía el tamaño de la tablas de direccionamiento. Se presentaron nuevas aproximaciones a la agregación de direcciones (en particular CIDR, *Classless Interdomain Routing*, enrutamiento entre dominios sin clase) para controlar el tamaño de las tablas de enrutamiento.

Como resultado del crecimiento de *Internet*, se produjo un cambio de gran importancia para la red y su gestión. Para facilitar el uso de *Internet* por sus usuarios se asignaron nombres a los *hosts* de forma que resultara innecesario recordar sus direcciones numéricas. Originalmente había un número muy limitado de máquinas, por lo que bastaba con una simple tabla con todos los ordenadores y sus direcciones asociadas. El cambio hacia un gran número de redes gestionadas independientemente (por ejemplo, las LAN) significó que no resultara ya fiable tener una pequeña tabla con todos los *hosts*. Esto llevó a la invención del DNS (*Domain Name System*, sistema de nombres de dominio) por *Paul Mockapetris* de USC/ISI. El DNS permitía un mecanismo escalable y distribuido para resolver jerárquicamente los nombres de los *hosts* (por ejemplo, www.acm.org) en direcciones de *Internet*.

En **1987** el número de *hosts* en *Internet* supera los 10.000 mientras que *Apple Computer* introduce *HyperCard*, el primer programa de hipermedia para usuarios.

El 1 de noviembre de **1988** *Internet* es atacada con un virus de tipo "gusano". Hasta el 10% de todos los servidores conectados fueron afectados. El acontecimiento subrayó la falta de adecuados mecanismos de seguridad en *Internet*, por lo cual DARPA formó el *Computer Emergency Reponse Team* (CERT), un equipo de reacción rápida que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.

En **1988** *Jarkko Oikarinen* escribe la que se considerará una de las populares aplicaciones en *Internet* conocida como IRC. Durante este año se completa el primer tendido transatlántico de fibra óptica entre los EE.UU. y Europa con una capacidad de transmisión de 40.000 llamadas telefónicas simultáneas.

- Este año un comité del *National Research Council* (Consejo Nacional de Investigación), presidido por *Kleinrock* y entre cuyos miembros estaban *Clark* y *Kahn*, elaboró un informe dirigido a la NSF y titulado *"Towards a National Research Network"*. El informe llamó la atención del entonces senador *Al Gore* quien le introdujo en las redes de alta velocidad que pusieron los cimientos de la futura Autopista de la Información.

Durante **1989** la empresa *Compuserve Information Service* lanza el primer servicio interactivo de información a través de computadores conectados a la *Ohio State University* contando con 1.200 abonados, menos de 20 años más tarde las redes globales de computadores que formarán *Internet* contarán con 40 millones de usuarios, el 70% de ellos en EE.UU.

En **1989** *Tim Berners-Lee* presenta una propuesta que contempla un sistema de hipertexto para permitir compartir la información en línea entre los investigadores de la *High Energy Physics Community*.

En **1990** ARPANET deja de existir. El protocolo TCP/IP había sustituido o marginado a la mayor parte de los restantes protocolos de grandes redes de ordenadores e IP estaba en camino de convertirse en el servicio portador de la llamada Infraestructura Global de Información. *Tim Berners-Lee* concreta el primer programa para navegar en la *web*.

- Durante este año se crea *The Electronic Frontier Foundation* (EFF) y diversos países como España, Argentina, Austria, Brasil, Chile, Irlanda, Suiza y Corea del Sur se conectan también a NSFNET desde el ámbito científico y académico.

Durante **1991** *Tim Berners-Lee* crea la *World Wide web*, utilizando tres nuevos recursos: HTML (*Hypertext Markup Language*), HTTP (*Hypertext Transfer Protocol*) y un programa cliente, llamado *web*

Browser. Todo este trabajo se basó en un escrito de *Ted Nelson*, en 1974, donde, por primera vez, se habló de *Hypertext* y *links*.

En **1991** se retiran las restricciones de NFS al uso comercial de *internet*. Ese mismo año también se conectan nuevos países a la NSFNET incluyendo: Croacia, Hong Kong, República Checa, Sudáfrica, Singapur, Hungría, Polonia, Portugal, Taiwan y Túnez.

En **1993**, la *National Science Foundation* crea INTERNIC (*Internet Network Information Center*), una especie de centro administrativo para *Internet* a fin de proveer acceso via *ftp*, *gopher*, *wais*, *e-mail* etc. servicios de registro de dominios y un directorio de recursos de *Internet*.

Durante 1993 el número de servidores *internet* sobrepasa los 2.000.000. También NSF patrocina la formación de una nueva organización, INTERNIC, creada para proporcionar servicios de registro en *Internet* y bases de datos de direcciones. En este año en el *National Center for Supercomputing Aplications* (NCSA), en la Universidad de Illinois, *Mac Andreessen* junto con un grupo de estudiantes crean un programa llamado *Mosaic* (*web Browser*), el cual ganó fama rápidamente. *Mac Andreessen*, al poco tiempo, se alejo del NCSA y junto con *Jim Clark* (fundador y renunciante de *Sylicon Graphics*) fundan *Netscape*. Aparece la aplicación *WinSock 1.1* estandarizando las posibilidades de aplicaciones Windows basadas en aplicaciones TCP/IP.

En **1994** *David Filo* y *Jerry Yang* crean el directorio-buscador de *Internet YAHOO!* (*Yet Another Hierarchical Officious Oracle*).

También en el año 1994 el número de servidores de *Internet* alcanza los 3.800.000. Las primeras tiendas *Internet* empiezan a aparecer junto con "emisores" de radio *on-line*. El conflicto potencial entre los internautas tradicionales y los nuevos usuarios se manifestó con fuertes protestas ante la aparición de publicidad en *Internet*, como avisos ostensibles en algunas páginas y el comienzo de lo que se conocerá como *Spam* (correo basura).

En **1995** hay más de 5 millones de servidores conectados a *Internet*. La espina dorsal de NSFNET (red académica de la *National Science Foundation*) empieza a ser sustituida por proveedores comerciales interconectados. La política de privatización de la NSF culmina con la eliminación de la financiación del *backbone* NSFNET. Los fondos así recuperados fueron redistribuidos competitivamente entre redes regionales para comprar conectividad de ámbito nacional a *internet* a las ahora numerosas redes privadas de larga distancia.

En EE.UU. es descatalogado el área de telefonía domestica mediante el Acta de Reforma de las Telecomunicaciones abriendo la competencia plena. Sus disposiciones incluyen un anexo conocido como *Communications Decency Act* (CDA), la cual motiva resistencias y terminará siendo declarada inconstitucional en 1997 [06].

2.3.2. Historia de las Redes Sociales

Debemos remontarnos al año **1995** cuando *Randy Conrads* crea el sitio *web Classmates.* Con esta Red Social se pretendía que los usuarios pudiesen recuperar o mantener el contacto con antiguos compañeros del colegio, instituto, universidad, etc.

En **1997** se pone en marcha el portal *web SixDegrees* el cual permitía a los usuarios crear perfiles, lista de amigos y amigos de sus amigos.

Entre los años **1997** a **2001** surgieron nuevos sitios de Redes Sociales como *AsianAvenue*, *Blackplanet*, y *MiGente* que dejaban a los usuarios crear relaciones personales y profesionales, creando perfiles que posibilitaban el que los usuarios identificaran a sus amigos en sus redes sin pedir la aprobación de esas conexiones.

En el año **2001** se creó el portal *Ryze* para ayudar a las personas a aprovechar sus objetivos empresariales y profesionales mediante la creación de redes profesionales. Su premisa fue proporcionar una red de apoyo para los consumidores en un entorno profesional que les permitiera la búsqueda de puestos de trabajo, hacer las conexiones de empresas, y potenciar las comunidades virtuales para las necesidades de las empresas en general.

Dos años más tarde en **2003** nació *LinkedIn* creada para capturar el mismo segmento de mercado que la mencionada *Ryze*. *LinkedIn* ha evolucionado hasta ser el estándar de la industria profesional para la creación de redes con muchas de las características de Redes Sociales adoptadas en el sitio. En la actualidad posee más 135 millones de usuarios registrados en más de 200 países distintos, que abarcan cerca de 170 empresas.

En **2003** comenzó también su andadura *MySpace*, se trata de un sitio *web* de interacción social constituido por perfiles personales de usuarios que incluye redes de amigos, grupos, *blogs*, fotos, vídeos y música, además de una red interna de mensajería que permite comunicarse a unos usuarios

con otros y un buscador interno. Se ha diferenciado de otros sitios *web* porque permite a los usuarios personalizar sus páginas.

En el año **2004** el estudiante *Mark Elliot Zuckerberg* de la universidad de *Harvard* crea una de las más famosas Redes Sociales llamada *Facebook*. Originalmente se creó para apoyar a las redes universitarias, y los usuarios del sitio estaban obligados a proporcionar las direcciones de correo electrónico asociada con las instituciones educativas. Posteriormente se amplió para incluir a los estudiantes de secundaria, profesionales, y finalmente todos los usuarios potenciales de *Internet*.

A diferencia de otras Redes Sociales, en *Facebook* los usuarios sólo pueden hacer públicos sus perfiles a otros usuarios del sitio.

Otra característica que distingue a *Facebook* es la capacidad para desarrolladores externos de crear aplicaciones lo que permite a los usuarios personalizar sus perfiles y realizar otras tareas, tales como comparar las preferencias de las películas.

A principios de **2008** lanzó su versión en francés, alemán y español para impulsar su expansión fuera de Estados Unidos, ya que sus usuarios se concentran en Estados Unidos, Canadá y Gran Bretaña.

Existen otras muchas Redes Sociales muy populares como:

- *Tuenti* que fue creada en 2006 por *Zaryn Dentzel*, un estudiante estadounidense actualmente afincado en Madrid (España). Se trata de una Red Social de acceso restringido a la que sólo se entra mediante la invitación de un miembro anteriormente registrado. Este mecanismo, según la empresa, garantiza en principio que todo usuario recién llegado ya tenga un vínculo con otro miembro de la red, a partir del cual pueda empezar a establecer relaciones con el resto de los usuarios.
- *Twitter* también creada en 2006, se define como una Red Social con servicio de *microblogging* que permite a sus usuarios enviar y leer mensajes breves de texto de una longitud máxima de 140 caracteres denominados como *tweets*. El envío de estos mensajes se puede realizar tanto por el sitio *web* de *Twitter*, como vía SMS (*short message service*) desde un teléfono móvil, desde programas de mensajería instantánea, o incluso desde cualquier aplicación de terceros, como puede ser *Twidroid*, *Twitterrific*, *Tweetie*, *Facebook*, *Twinkle*, *Tweetboard* o *TweetDeck* [07].

2.4. Ventajas e inconvenientes de las Redes Sociales

Las principales ventajas e inconvenientes comunes a toda Red Social a nivel de perfil personal:

VENTAJAS	INCONVENIENTES
- Gran medio de comunicación, además de poder ser en tiempo real.	- Invasión de la privacidad.
- Excelente para propiciar contactos afectivos nuevos como: búsqueda de trabajo, amistad o compartir intereses sin fines lúdicos.	- Sensación de falta de seguridad en cuanto al control de la información publicada.
- Diluyen las fronteras geográficas.	- Posible adicción.
- Puede generar movimientos de solidaridad ante una situación de crisis. Gran medio mediático.	
- Nuevo poder mediático.	

Y desde el perfil profesional y de negocio:

VENTAJAS	INCONVENIENTES/PELIGROS
- Gran medio para la publicidad tanto del profesional que busca empleo como de la empresa que oferta servicios y/o productos.	- Los malos comentarios en la red pueden dar mala imagen al negocio.
- Han modificado la manera de hacer marketing, generando una mayor segmentación de medios e interactividad con sus consumidores	- Los mensajes han de ser muy directos y escuetos.
- Perfectas para establecer conexiones con el mundo profesional.	- Los empleados pueden hacer uso no profesional de las Redes Sociales.
- El consumidor puede interactuar y conocer las características de los productos, además de promociones, noticias de la empresa, lanzamiento de nuevos productos, etc.	

A continuación se explican las más reseñables:

Gran medio de comunicación

En primer lugar debemos diferenciar dos tipos de comunicación que se pueden dar en la inmensa mayoría de las Redes Sociales y en *Internet* en general:

- Comunicación Síncrona: Es el intercambio de información por *Internet* en tiempo real. Es un concepto que se enmarca dentro de la CMC (*computer mediated comunication*), que es aquel tipo de comunicación que se da entre personas y que está mediatizada por ordenadores. Ejemplo: *Chat* [08].
- Comunicación Asíncrona: Es aquella que permite la comunicación por *Internet* entre personas de forma no simultánea. Ejemplo: *e-mail* [08].

Las Redes Sociales se han convertido en un gran medio de comunicación. Es el auge del periodismo ciudadano donde cualquiera puede publicar una información, sea o no periodista, trabaje o no en un medio de comunicación. Esto es así no sólo con las Redes Sociales de noticias, donde se envía la información y se vota en función de su interés, también las redes de amigos son un foro para trasmitir las noticias. Se ha descubierto una nueva forma de comunicarse y las Redes Sociales superan ya al correo electrónico. Los usuarios de las Redes Sociales consumen alrededor del 10% del tiempo que dedican a navegar, una cifra que ya supera los minutos dedicados por los internautas al correo electrónico, según el último registro realizado por la empresa de medición de audiencias en la red, *Nielsen Online* [09].

Publicidad

Las Redes Sociales se están convirtiendo en una de las herramientas más importantes del *marketing* en las empresas de cualquier sector.

Estos nuevos medios de comunicación han revolucionado por completo el mundo de la publicidad online. Se trata de una herramienta sumamente útil para las empresas, puesto que gracias a ella tienen la posibilidad de encontrar y establecer una relación más personalizada y dinámica con su público potencialmente objetivo.

Las empresas son conscientes de que se están convirtiendo en uno de los principales canales de comercialización y de comunicación, por lo que en un espacio corto de tiempo se ha aumentado notablemente la cantidad de dinero que se destina a la inversión publicitaria en *Internet*.

Una de las mayores ventajas que este tipo de espacios proporcionan, es la creación de un clima de mayor confianza entre la empresa y los clientes, gracias a la comunicación dinámica que se genera entre ambos.

Este clima de confianza con los clientes se consigue mediante contenidos especializados en diferentes temáticas.

Con el vasto intercambio de información entre empresa y clientes se va creando un canal de comunicación segura entre ambos, por lo que poco a poco el usuario irá adquiriendo más confianza en la información que recibe y estará más dispuesto a valorar como interesante y/o relevante la información que recibe a través de nuestra cuenta en la Red Social [10].

La invasión de la Privacidad

Al utilizar las Redes Sociales es muy común que se solicite la creación del perfil. En algunos casos se puede mentir, pero lo cierto es que el fin de las Redes Sociales de amigos, por ejemplo, es el de socializarte, encontrar a amigos que hace tiempo que no veías, intercambiar opiniones con otros compañeros... Y no tiene mucho sentido si no se sabe quién es cada uno.

Figura 2. Noticia de espionaje en Facebook [REF_FIG2].


Espionaje entre trabajadores a través de Facebook

La mitad de los empleados españoles con un perfil en las redes sociales no protege su intimidad, según un estudio

facebook

Y si incluyes el perfil, incluyes tus datos personales, tu fotografía, tu fecha de nacimiento... todo aquello que te distingue como persona y te diferencia de los demás. Es como publicar tu DNI, exponer al público todo lo que eres. Y ¿hasta qué punto sabemos que todos tus datos no se van a utilizar para otros fines? Muchos anunciantes están siempre esperando conocer la información de sus potenciales

clientes, y las Redes Sociales tienen esos datos tan suculentos para las empresas anunciadoras. Esta situación está provocando que haya empleos en los que se espíe a los trabajadores, se entra en una Red Social para conocer qué es lo que hace y ver el tiempo consumido en horas de trabajo. Las Redes Sociales también están sirviendo para conocer a la persona que se postula a un puesto de trabajo antes de conocerla personalmente. Y esto puede cambiar la balanza hacia un lado o hacia otro de la decisión de contratarle.

La falta de Seguridad

Unido a esta exposición pública de la privacidad de los usuarios de las Redes Sociales, está la falta de seguridad. Hay demasiada información personal rodando por ahí, y pocas garantías de que esté bien resguardada. Recientemente se ha dado a conocer que miles de *hackers* (se define como la/s persona/s que realizan actividades delictivas con ayuda de redes de comunicaciones y sistemas informáticos electrónicos o contra tales redes y sistemas), contaban con cuentas en *Facebook*. Esta delincuencia pone de manifiesto que en una comunidad tachada de segura, miles de personas acusadas de abusos sexuales continúan manteniendo relaciones virtuales en la red.

Un macabro delito sexual fue el perpetrado por *Anthony Stancl*, el cual se hizo pasar por chicas de instituto que ligaban con chicos menores de edad, convenciéndoles para que le enviasen fotos desnudas. Una vez que el joven, de 18 años, tenía las imágenes en su poder chantajeaba a los adolescentes, obligándoles a mantener relaciones sexuales con él. *Facebook* rápidamente reaccionó afirmando que sólo existían menos de un 1% de cuentas falsas [11].

La participación en las Redes Sociales no está exenta de riesgos, como la suplantación de identidad digital. Incluso los usuarios más cuidadosos pueden entregar información personal a extraños sin que se den cuenta, al bajar e instalar una aplicación diseñada por terceros y que incluyen juegos, competencias, concursos de conocimientos y regalos virtuales. Las personas que ingresan a estas redes piensan que esa información, que considera privada, pueden verla solo los amigos o grupos específicos, pero los programadores a veces la utilizan para poner en contacto a usuarios con intereses parecidos. Otras veces se usa para difundir publicidad orientada a sectores específicos, tomando en cuenta cosas como la edad y el género.

La Adicción

Con el desarrollo de *Internet* y su crecimiento exponencial, según las Naciones Unidas, *Internet* registra una tasa de crecimiento anual de cerca del 30%, con el 2,5% de la población mundial sumándose año tras año a sus usuarios, han aparecido también los primeros casos de psicopatología relacionados con *Internet* y en concreto con las Redes Sociales. El trastorno de dependencia a *Internet* en general se ha conocido con muchos nombres: ódesorden de adicción a *Internet*ôï *Internet Addiction Disorder* (IAD)ï (*Goldberg*, 1995), óuso compulsivo de *Internet*ô(*Morahan-Martin* y *Schumacker*, 1997), o óuso patológico de *Internet*ôï *Pathologica*l *Internet* Use (PIU)- (*Young y Rodgers*, 1998b) ï [12].

La tarea de definir lo que es la adicción a *Internet* y a las Redes Sociales en concreto es algo que ya de partida supone un problema para muchos psicólogos.

Las nuevas tecnologías permiten que con un solo *clic* la persona pueda desinhibirse rápidamente, crear identidades falsas o dar una imagen propia que no corresponde con la realidad.

La adicción a las Redes Sociales suele afectar a las personas que psicológicamente o por la edad son más vulnerables. Un grupo al que hay que prestar especial atención son los adolescentes porque reúnen características de riesgo: impulsividad externa, necesidad de relaciones nuevas y autoestima baja. Uno de los indicadores más claros de que se está cayendo en una dependencia es la imposibilidad de controlar el tiempo que se quiere estar conectado y la única terapia frente a esta adicción es evitar los factores de riesgo. "Si son adolescentes, no deben tener ordenador en su habitación; tampoco deben navegar solos. Es muy importante hacer ver al afectado que tiene una adicción lo antes posible. Los padres que no consiguen reconducir la situación deben acudir a su médico de primaria o a un pediatra para que, en los casos más graves, puedan derivar al adolescente a un centro de salud mental donde tenga la posibilidad de ser tratado por psicólogos clínicos o psiquiatras."

2.5. Tipología y ejemplos de Redes Sociales

Las Redes Sociales se pueden categorizar atendiendo a los usuarios a los que se dirigen, o al tipo de contenido que albergan. De esta manera, se distinguen, dos grandes grupos de Redes Sociales, las de ocio y las profesionales.

A pesar de que cada tipo presenta una serie de aspectos singulares, ambos grupos cuentan con una serie de características básicas y estructurales en común:

- Tienen como finalidad principal poner en contacto e interrelacionar a personas. La plataforma facilita la conexión de forma sencilla y rápida.
- Permiten la interacción entre todos los usuarios, ya sea compartiendo información, facilitando el contacto directo o proponiendo nuevos contactos de interés.
- Fomentan la posibilidad de que los usuarios inicialmente contactados a través del medio *online* acaben entablando un contacto real.
- Impulsan un contacto entre usuarios ilimitado, en la medida en la que el concepto espacio y tiempo se convierte en relativo, al poder comunicar desde y hacia cualquier lugar, así como en cualquier momento, con la única condición de que ambas partes acepten relacionarse entre sí.
- Fomentan la difusión viral de la Red Social, a través de cada uno de los usuarios que la componen, empleando este método como principal forma de crecimiento del número de usuarios.

2.5.1. Redes Sociales de Ocio

Su objetivo principal radica en el hecho de facilitar y potenciar las relaciones personales_entre los usuarios que la componen. El grado de crecimiento de estas redes ha sido muy elevado en los últimos años, llegando a constituirse plataformas como el ya mencionado portal *Facebook*.

Según muestran los datos de los últimos estudios realizados en el sector este tipo de redes complementa, e incluso sustituye, especialmente en el rango de edad de usuarios más jóvenes, a otros medios de comunicación como la mensajería instantánea, ampliamente utilizada durante los últimos años. Este hecho se debe en gran medida a los aspectos que caracterizan a las Redes Sociales de ocio:

- Ofrecen gran variedad de aplicaciones y/o funcionalidades que permiten a los usuarios prescindir de herramientas de comunicación externas, poniendo a su disposición una plataforma que integra todas las aplicaciones necesarias en una misma pantalla.
- Fomentan que los usuarios no se centren únicamente en operar de forma online, sino que este medio sirva de plataforma para convocar y organizar aspectos de su vida cotidiana.

- Ponen a disposición de la comunidad de usuarios parte del código24 usado para programar la plataforma, de modo que los usuarios puedan desarrollar aplicaciones propias, que sean ejecutadas dentro de la Red Social, o aplicaciones externas que se interconecten con la plataforma, logrando así el aumento de la utilidad y con ello de la difusión.

Dentro del amplio abanico de Redes Sociales generalistas o de ocio, se puede establecer, al menos, tres subdivisiones atendiendo a la finalidad o temática de las mismas:

- Plataformas de intercambio de contenidos e información:

  Servicios como *Youtube*, *Dalealplay*, *Google* Vídeo, etc., que se caracterizan principalmente por la puesta a disposición de los usuarios de herramientas gratuitas y sencillas para el intercambio y la publicación de contenidos digitales (vídeos, fotos, textos, etc.).

  En sentido estricto, no se puede considerar que este tipo de plataformas sean Redes Sociales, ya que únicamente permiten el alojamiento de contenidos para que el resto de usuarios puedan visionarlo, limitándose la interacción entre los usuarios a la posibilidad de incluir comentarios respecto a los contenidos y otorgar puntuaciones a los mismos.

  No obstante, y aunque estas plataformas eran inicialmente independientes de las Redes Sociales, permiten actualmente enlazar los contenidos y publicarlos directamente en el perfil de la red utilizada por el usuario.

- Redes Sociales basadas en perfiles:

  Redes como *Facebook*, *Tuenti*, *Wamba*, *Orkut*, etcé Este tipo de servicio es el más utilizado en *Internet* por encima de cualquier otro tipo de Red Social y es además el más representativo dentro del grupo de Redes Sociales de ocio.

  Las aplicaciones que terceros están desarrollando para algunas de estas redes permite que ofrezcan cada vez un mayor número de posibilidades, lo que, unido a su idiosincrasia está sustituyendo al uso de herramientas de comunicación tradicionales en *Internet*.

  Este tipo de redes con frecuencia se encuentra dirigido a temáticas concretas, creando grandes comunidades de usuarios con altos niveles de especialización en determinados temas. De este modo, se constituyen como fuentes de información y conocimiento.

- Redes Sociales de *Microblogging* o *Nanoblogging*:

  Plataformas como *Twitter* o *Yammer*. Este tipo de redes basan su servicio en la actualización constante de los perfiles de los usuarios mediante pequeños mensajes de texto, que no superan los 140 caracteres. Esto permite poner a disposición del resto de usuarios información clara, concisa, sencilla y rápida sobre las actividades que se están realizando en ese momento, impresiones, pensamientos, publicaciones, etc.

  Todas las actualizaciones son mostradas el perfil del usuario y al mismo tiempo son publicadas en la página *web* de seguimiento de otros usuarios. [13].

2.5.2. Redes Sociales de contenido profesional

Se configuran como nuevas herramientas de ayuda para establecer contactos profesionales con otros usuarios. Entre ellas se encuentran *web*s como ô*Xing*ôo ô*Linkedn*ôy constituyen el segundo gran bloque de Redes Sociales.

Están creadas y diseñadas con la finalidad de poner en contacto y mantener la relación a nivel profesional con diferentes sujetos que tengan interés para el usuario. Es por ello que la edad es un factor determinante en el uso de estas redes. Las redes de contenido profesional apenas son utilizadas por los menores de 20 años, incrementándose el porcentaje de usuarios a medida que aumenta su edad. De manera inversa, el porcentaje de usuarios de las Redes Sociales de ocio disminuye con la edad o sufre una migración desde las redes más orientadas a adolescentes (*Tuenti* o *Fotolog*) hacia otras con mayor número de servicios (*Facebook*).

Así, entre las principales utilidades cabe citar:

- Desde el lado del trabajador: La búsqueda de nuevas oportunidades de empleo, el establecimiento de nuevos contactos profesionales o la promoción laboral. Permiten a los usuarios entrar en contacto con otros profesionales de su sector a través de conocidos comunes de confianza, ayudando a mejorar las conexiones con otras personas que, en circunstancias habituales, serían inaccesibles debido a su cargo o responsabilidad.
- Desde el lado de la empresa: La presencia en este tipo de Redes Sociales resulta cada vez más importante, ya que las empresas utilizan este nuevo recurso para identificar posibles candidatos

participantes en sus procesos de selección o profundizar en la información disponible del perfil de los candidatos seleccionados en un proceso de contratación determinado [13].

Este tipo de redes está en auge. En el año 2007 se consolidaron como uno de los servicios de mayor crecimiento, produciéndose durante los meses de junio y julio grandes fusiones e inversiones económicas en el sector.

Los beneficios que este tipo de Redes Sociales de carácter profesional pueden reportar al entorno empresarial no radican exclusivamente en servir como herramienta complementaria en un proceso de selección de personal, ni se quedan en las posibilidades que evidencian los datos indicados, sino que además resultan especialmente atractivas como alternativa de negocio, ya que permiten:

- La realización de acciones de marketing personalizado.
- La creación de servicios Premium de suscripción.
- La publicación de contenidos de interés general y la promoción de contenidos propios.
- La venta de bonos de ñaumento de confianza del usuarioñ Se trata de una especie de certificación proveniente de la propia Red Social que asegura que el usuario es de confianza y que sus finalidades no son mal intencionadas.

En particular, el uso de los servicios *premium* en este tipo de redes, a diferencia de otro tipo de plataformas, dispone de un alto rendimiento del número de usuarios, que abonan una cantidad mensual, para acceder a servicios avanzados.

Las principales ventajas del uso de este tipo de Redes Sociales para las empresas son:

- Acceso inmediato a los servicios sin necesidad de adquirir *hardware* o *software*.
- Pertenencia por parte de los trabajadores a una misma comunidad lo que conducirá a un mejor ambiente de trabajo.
- Facilidad para la captación de nuevos clientes.
- Costes anuales potencialmente inferiores debido al uso de servicios.
- Ventajas provenientes de una conexión a Internet.

Mención especial tienen las *Redes Sociales* de contenido profesional orientadas a la enseñanza y que están suponiendo una innovación didáctica. Entre ellas podemos destacar:

LiveMocha: Completa comunidad con muchos cursos de distintos niveles y un gran número de lenguas para elegir.

Babbel: Su principal actividad consiste en el intercambio de ejercicios de adquisición de vocabulario para el aprendizaje de idiomas.

Cabe destacar que existen también Redes Sociales Mixtas, tales como *Yuglo, Unience, PideCita*, en las que ofrecen a los usuarios y a las empresas desarrollar tanto actividades de ocio como de negocio [13].

2.6. Perspectiva futura de las Redes Sociales

El elemento fundamental para el desarrollo y futuro de la Redes Sociales son los Medios de Comunicación Sociales (*Social Media*). El *Social Media* es un término de marketing que hace referencia a la estrategia y conjunto de acciones llevadas a cabo en las Redes Sociales con una finalidad publicitaria o comercial. El término fue creado por *Rohit Bhargava* y debido a la proliferación de las Redes Sociales, el tiempo que los usuarios pasan en ellos y los beneficios que aporta en términos de tráfico y posicionamiento en buscadores ha adquirido una gran relevancia por parte de empresas y expertos en *marketing* digital.

Por tanto el *Social Media*, tiene como objetivo apoyar a los profesionales y a las empresas, optimizando y conociendo las mejoras estratégicas de *marketing*, para la gestión de sus Redes Sociales y comunidades *online.*

Por otro lado el surgimiento de nuevas Redes Sociales especializadas está en auge. La ventaja de estas frente a las generalistas de cara a su rentabilidad, es que las Redes Sociales permiten segmentar a los usuarios en función de dicha especialización, algo que no ocurre en redes como *Twitter*, *Facebook*, etc. Las Redes Sociales especializadas están en su infancia y las generalistas estarían captando una parte importante del mercado [14].

CAPÍTULO 3

SEGURIDAD EN LAS REDES SOCIALES

3. SEGURIDAD EN LAS REDES SOCIALES

3.1. La seguridad en las Redes Sociales

En los últimos tiempos, los servicios de Redes Sociales han experimentado gran auge entre el público. Entre otras cosas, estos servicios ofrecen medios de interacción basados en perfiles personales que generan sus propios usuarios registrados, lo que ha propiciado un nivel sin precedentes de divulgación de información de carácter personal de las personas interesadas y de terceros.

Aunque los servicios de Redes Sociales aportan un amplio abanico de oportunidades de comunicación, así como el intercambio en tiempo real de todo tipo de información, la utilización de estos servicios puede plantear riesgos para la Privacidad de sus usuarios. La Privacidad en *Internet* se refiere a controlar quien puede tener acceso a la información que posee un determinado usuario que se conecta a *Internet*. Los datos personales relativos a las personas son accesibles de forma pública y global, de una manera y en unas cantidades sin precedentes, entre las que se incluyen enormes cantidades de fotografías y vídeos digitales.

Esta violación de la Privacidad atenta en mayor o menor medida contra los derechos constitucionales, que citamos a continuación y que la propia Constitución Española (CE) de 1978 establece para cada uno de estos bienes, derechos y libertades de los ciudadanos y que extenderemos en el apartado 4:

- La protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- La protección de datos de carácter personal.
- La protección de la producción y creación literaria, artística, científica y técnica mediante los instrumentos reguladores de la propiedad Intelectual e Industrial de las Obras.
- La protección de los derechos de consumidores y usuarios.

Como hemos citado, las páginas de Redes Sociales, nos permiten tener una imagen de nuestra Red Social, pero a menudo también son un lugar para la publicación de información que se puede considerar confidencial. Por tanto, las personas se enfrentan a posibles pérdidas de control sobre la forma en que terceros emplearán nuestra información una vez publicada en la red.

Aunque la base ódecomunidadô de las Redes Sociales sugiere que la publicación de los datos personales de carácter privado sería comparable a compartir información con amigos de forma

presencial, en realidad la información de cada perfil está disponible para toda una comunidad de usuarios que pueden ascender a millones.

Actualmente, existe muy poca protección frente a la copia de todo tipo de datos personales en estos perfiles (por parte de los miembros de la red o de terceras personas sin autorización y ajenas a la red), así como frente a su utilización para crear perfiles personales o volver a publicar dichos datos en cualquier otro lugar. Puede resultar muy arduo (y en ocasiones, imposible) eliminar por completo determinada información una vez que ha sido publicada en *Internet*: incluso una vez que ha sido eliminada del sitio original, es posible que terceras partes o los propios proveedores de los servicios de Redes Sociales conserven copias. Los datos de carácter personal procedentes de perfiles también pueden filtrarse fuera de la red cuando son indexados por motores de búsqueda. Además, algunos proveedores de servicios de Redes Sociales facilitan datos de los usuarios a terceras partes a través de ñinterfaces de programación de aplicacionesò, que, en ese momento, pasan a ser controlada por dichas terceras partes.

Un ejemplo de usos secundarios que ha captado la atención del público es la práctica de responsables de personal de algunas empresas que investigan los perfiles de candidatos a un puesto de trabajo o incluso de empleados: según algunos informes de prensa, un tercio de los responsables de recursos humanos admite emplear datos de servicios de Redes Sociales en su trabajo para comprobar y/o completar detalles de los candidatos a un puesto de trabajo.

Los proveedores de servicios de Redes Sociales también utilizan la información de los perfiles y de los datos sobre tráfico para emitir mensajes de marketing personalizado a sus usuarios. Es muy probable, que en el futuro, surjan otros usos no esperados de la información contenida en los perfiles de usuarios.

La 30º Conferencia Internacional de Autoridades de Protección de Datos y de privacidad recuerda que estos riesgos ya se han analizado en el ñ*Report and Guidance on Privacy in Social Network Services*ò (Informe y asesoramiento sobre la privacidad en los servicios de Redes Sociales), así como en el Documento de posición nº 1 de ENISA ñ*Security Issues and Recommendations for Online Social Networks*ò(Problemas y recomendaciones de seguridad aplicados a las Redes Sociales en línea) [15].

Las Autoridades de protección de datos y privacidad reunidos en la Conferencia Internacional están convencidos de la necesidad de realizar, en primera lugar, una amplia campaña de información en la que participen actores públicos y privados (desde organismos gubernamentales a instituciones educativas, desde proveedores de servicios de Redes Sociales a asociaciones de consumidores y

usuarios, así como las propias Autoridades de protección de datos y de privacidad) de cara a impedir los muy diversos riesgos asociados con el uso de los servicios de Redes Sociales.

3.2. Factores que afectan a la seguridad

Como hemos comentado en el apartado anterior la principal inseguridad en las Redes Sociales viene ligada a la violación de la privacidad de los datos (fotos, videos, datos personales, datos profesionales, etc.) de los usuarios de las mismas.

Las tres fases de riesgo para la privacidad y la seguridad de la información de los usuarios a la hora de utilizar una determinada Red Social son:

1. En el momento de registrarse: donde normalmente nos encontramos formularios muy amplios, complicados y que demandan información, donde en ocasiones ya estamos desvelando datos relativos a la ideología política, orientación sexual o preferencia religiosa y más aún, aceptamos las condiciones de privacidad con aún muchísimas lagunas legales, entre las más negativas, el proveedor es propietario del contenido de su red. Otro factor negativo es el referente a la publicidad del perfil, donde por defecto viene activado todo, es decir, el nivel mínimo de seguridad y máxima exposición.

2. Durante el desarrollo de la actividad en la red: el posible riesgo que conlleva la publicación y exposición de información personal normalmente, excesiva, tanto la propietaria como de terceros, en este último, sin que se recoja por ningún sitio el consentimiento de estas publicaciones. Existen otros riesgos como los motores de indexación (opciones de búsqueda de las propias Redes Sociales por nombre, aficiones, ciudad, etc.) que tienen estos servicios, exponiendo ya inicialmente mucha información de los usuarios. Finalmente, un riesgo muy crítico es el de la suplantación de la identidad (*Phishing*) y la generación de *Spam* o correo basura a partir de nuestras listas de direcciones que incluimos en nuestro perfil.

3. Al darse de baja del servicio: donde resulta difícil, por no decir imposible, conseguir una baja efectiva del servicio ya que parte de los datos de los usuarios pueden seguir publicados en los perfiles de otros usuarios de la red, y porque existen grandes lagunas legislativas entre la propiedad de nuestra información por parte de los proveedores y los plazos en lo que se conserva dicha información desde que un usuario se da de baja del servicio.

Diferentes estudios demuestran que los usuarios de las Redes Sociales no les preocupan los riesgos que podrían implicar la publicación de sus datos en las Redes Sociales. Esta actitud se debe a que los usuarios no conocen los potenciales riesgos a su privacidad, asumen que las restricciones predispuestas por el sitio son suficientes para proteger sus datos personales y tienen la percepción que las Redes Sociales en *Internet* poseen menos riesgos que otras operaciones *on-line* (tal como, operaciones bancarias, compras, etc.) [16].

Por lo tanto, existe una falta de conocimiento generalizada entre los usuarios de Redes Sociales sobre los potenciales riesgos a su privacidad. Algunos de estos son:

- Creación de Dossiers Digitales por Terceros: Los perfiles construidos en las Redes Sociales pueden ser descargados y archivados por terceros, para generar bases de datos o dossiers digitales de los usuarios. Esto permite la generación de ficheros de datos sin autorización de los usuarios y se podrían utilizar los mismos para fines ilícitos (extorsión, calumnias, injurias, etc.).

- Recolección de Datos Secundarios: Más allá de los datos personales voluntariamente cargados a los perfiles, los usuarios también proveen información personal al responsable del sitio por el sólo uso de la Red Social: tiempo y duración de la visita al sitio, dirección IP, navegador utilizado, preferencias de uso, aplicaciones contratadas, etc. Esto le permite a los sitios personalizar la publicidad, adaptar sus servicios a las pautas de consumo de los usuarios y comercializar dicha información a terceros.

- Dificultad de Suprimir por completo los datos de la Cuenta del Usuario: Si bien las Redes Sociales permiten dar de baja el perfil, los comentarios, fotografías y otras informaciones de los usuarios persisten en los perfiles de los demás usuarios de la red. Asimismo, las Redes Sociales conservan copias archivadas de los perfiles por tiempo indeterminado. Esto dificulta la efectiva disposición de los usuarios de su propia información.

- *Spam*: Las Redes Sociales ya han sido víctimas del correo no solicitado. Los *Spammers* buscan ubicar su publicidad no solicitada a través de perfiles falsos, invitaciones de amigos falsos a través de perfiles muy atractivos, robo de contraseñas para enviar publicidades a todos los contactos, etc.

- Perfiles Falsos y ataques a la Reputación: La creación de perfiles con personas de renombre para deteriorar su reputación o la creación de perfiles de personas dentro de una determinada red para perjudicar su imagen.

- Persecuciones o *Ciberbullying* [26]: La realización de conductas amenazantes contra una víctima a través de medios electrónicos se ve facilitado por las Redes Sociales, al poner a disposición de los atacantes los datos personales, de localización y status online de los usuarios.

Por otra parte, se indica también que la propiedad intelectual (definición: La propiedad intelectual es un derecho patrimonial de carácter exclusivo que otorga el Estado por un tiempo determinado para usar o explotar en forma industrial y comercial las invenciones o innovaciones, tales como un producto técnicamente nuevo, una mejora a una máquina o aparato, un diseño original para hacer más útil o atractivo un producto o un proceso de fabricación novedoso; también tiene que ver con la capacidad creativa de la mente: las invenciones, las obras literarias y artísticas, los símbolos, los nombres, las imágenes y privilegios.) puede verse afectada como hemos mencionado anteriormente en el campo de las Redes Sociales. Tras la revisión de las condiciones de uso de las principales plataformas que operan en España, se ha constatado que es práctica general el que los avisos legales establezcan la cesión obligatoria de los derechos de propiedad intelectual de los contenidos generados por el usuario en favor de la plataforma o servidor de Redes Sociales. En este sentido, se hace hincapié en el hecho de que, al aceptar las condiciones de uso, el usuario puede estar cediendo plenamente sus derechos de explotación por los contenidos que publique a las plataformas, para que estas los utilicen libremente durante un plazo de 5 años.

No obstante, existe la posibilidad de ñdenunciar" aquellos contenidos que no cumplan con las condiciones de registro de la plataforma o que atenten tanto contra los derechos que ostentan los usuarios sobre sus obras de propiedad intelectual, como contra los de terceros. Para este cometido, existen mecanismos automáticos de autorregulación de los contenidos de los propios usuarios.

La compañía de seguridad *Verising iDefense* ha desvelado que un *hacker* ruso que actúa bajo el pseudónimo de *Kisloss* habría puesto en venta en *Internet* el acceso a 1,5 millones de cuentas de *Facebook*. Sus precios oscilan entre los 25 dólares por 1000 cuentas con 10 amigos o menos, o 45 dólares por 1000 cuentas con más de 10 amigos. (Noticia aparecida en el diario gratuito QUE¡ el 22 de Abril de 2010).

3.3. Amenazas y vulnerabilidades

No sólo hay que mencionar los riegos que se originan entre los usuarios de Redes Sociales en cuanto a su privacidad como hemos descrito sino también a las amenazas técnicas que permiten el acceso y el uso fraudulento a terceros de la citada información personal de los usuarios de estas redes. Estas

amenazas, (alguna descrita entre los riesgos anteriormente listados) corresponden no sólo al contexto de las Redes Sociales sino en general, a *Internet*, y que aprovechan el auge y la juventud de estas redes para realizar actos delictivos.

Un ejemplo de vulnerabilidad de estas Redes Sociales la encontramos en las aplicaciones de terceras empresas desarrolladas para utilizarse dentro de estos sitios con la finalidad de hacer más completa la experiencia de los usuarios. El desarrollo de aplicaciones de terceros para estos sitios *web* ha reducido los niveles de seguridad, tal y como ya ha ocurrido con la última inyección *SQL* detectada en *Facebook* y otras Redes Sociales como *MySpace*, por tanto, esta iniciativa también incide en un menor control de la seguridad que pueden encontrar en estas redes.

No en vano, se ha descubierto recientemente una inyección *SQL* en dos aplicaciones distintas dentro del subdominio *apps.Facebook.com*. Tal y como señalan *Nir Goldshlager* y *Rafel Ivgi*, especializados en seguridad, ñuno de los servidores está corriendo como *root*, lo que significa que se puede escribir ficheros dentro de la máquina y con grandes posibilidades de ejecutar código en el servidor con derechos de administrador. En estos casos, es posible obtener información acerca de los usuarios ya que la aplicación es capaz de obtener e insertar información maliciosa dentro de la base de datosò[16].

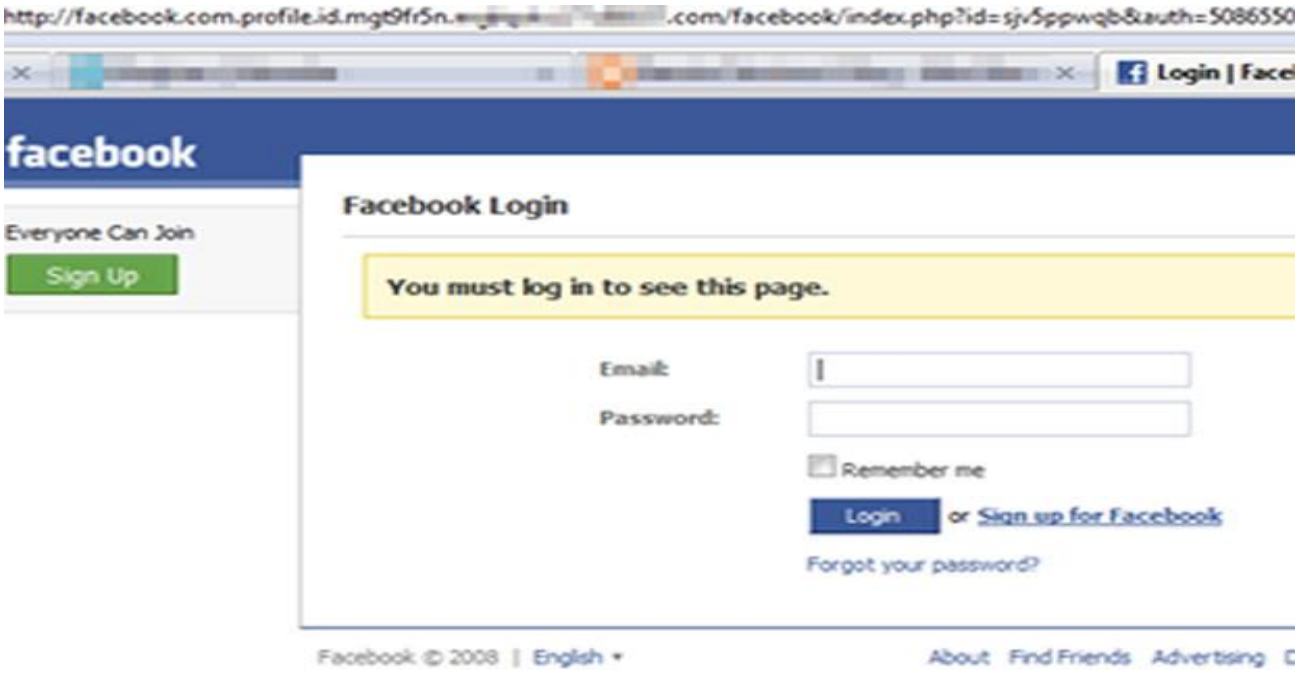
Aun así, los responsables de seguridad de *Facebook* han comentado que arreglar aplicaciones de terceros forma parte del trabajo de los desarrolladores que las han creado, y por tanto, el código de estas aplicaciones no se encuentra en los sistemas de *Facebook*. Aunque cuando se recibe un problema de vulnerabilidad en terceras aplicaciones automáticamente deshabilitan estos módulos hasta que se solucione el problema, existe un vacío legal de responsabilidades y sobre todo de seguridad [17].

En la actualidad, la crisis económica está agudizando el ingenio de los *hackers* y ya no sólo nos encontramos el conocido problema denominado **ataque de *Phishing*** aprovechando falsas noticias de quiebra de bancos, así como falsos portales con ofertas de empleo, sino que también las Redes Sociales también son objetivo de ataque.

Las acciones fraudulentas en estos sitios están relacionadas, como hemos citado, con el *Phishing*, con el fin de apoderarse de los usuarios. Estas amenazas adquirirán cada vez más importancia en las empresas debido a que los nuevos empleados acceden a menudo a estas herramientas utilizando los recursos corporativos [21].

En general, vemos que estas nuevas redes presentan también el creciente interés de ***Spammers*** y creadores de ***malware*** o programas maliciosos por las Redes Sociales, para aprovecharse de la confianza que generan, para enviar *Spam* y *malware*. Ejemplos de estos nos encontramos en la actualidad donde por ejemplo, *Facebook* y *Hi5* sufren un ataque exagerado de *phising* donde en las dos primeras horas, tras detectar el fraude, se localizaron 50 *web*s falsas que simulaban ser estas Redes Sociales.

Figura 3. Ventana falsa que replica el sistema de conexión a Facebook (Ref_Fig3).



Dentro de la propagación de estos *Spam*, normalmente dirigido al resto de usuarios de la red gracias a la recopilación de sus direcciones, propagan "*software* maligno", como los programas espías citados, que se infiltran para recopilar la información sobre las actividades llevadas a cabo en el ordenador de los usuarios y la obtención de datos de los mismos para su utilización ilegítima, todo ello potenciado **por la instalación y uso de *cookies* sin conocimiento del usuario** por parte del servicio, que permiten, entre otras cosas, almacenar información sobre el mismo y sus hábitos de navegación. De cara al usuario, aquí existen soluciones que, en general, se centra en deshabilitar algunas funcionalidades en los navegadores como la ejecución de componentes *JavaScript*, *Flash*, *plugins* o *ActiveX* entre otros. Otra opción menos agresiva sería aprovecharse de las extensiones que proponen los navegadores para evitar la ejecución de dichos componentes. Por ejemplo, en *Firefox*, se consigue instalando una

extensión llamada *NoScript*. En definitiva aprovechar la configuración de seguridad de nuestros navegadores.

Otro problema ya citado es el de la **suplantación de la identidad**, donde ya nos estamos encontrando numerosos casos denunciados en *Facebook* y otras Redes Sociales y que está obligando a los organismos tales como la Agencia Española de Protección de Datos (AEPD) y también el Instituto Nacional de Tecnologías de la Comunicación (INTECO) a iniciar una inspección sectorial de oficio a través de tres Redes Sociales --dos a nivel internacional y una "importante" *web* española, sin especificar--, para "verificar los niveles de riesgo" de estos espacios, y en particular, la espinosa situación legal para el caso de menores de edad. En este sentido, se observa la necesidad de una implantación de sistemas que faciliten la comprobación de la edad de los usuarios que intenten acceder al servicio, reduzcan los casos de suplantación de identidad (bloqueando el acceso al usuario que utilizó el perfil de otro de forma ilegítima) o detecten el nivel de seguridad de las contraseñas elegidas (e informen de los mínimos aconsejables), como siempre mejoras técnicas y recomendaciones que podrían complementarse con algún mecanismo de certificados para legitimar la autenticidad pero sin sacrificar en demasía la fluidez actualmente existente en la participación en las Redes Sociales, tal y como describe el artículo de las Redes Sociales y *OpenID* [19].

Se pueden encontrar preocupantemente otros muchos casos de este tipo, por ejemplo, otro casos de código malicioso de este tipo han sido detectado como refleja US-CERT (*Current Activity - Malicious Code Targeting Social Networking Site Users*) el cual confirma la penetración de este preocupante problema, donde apoyándose en una actualización de *Adobe Flash Player update*, introducen código malicioso en nuestros ordenadores.

En este sentido, este organismo informa de pautas a seguir, en general, aplicables para el acceso a *Internet* en general, para mitigar estos ataques, algunas de estas son:

a. Instale *software* antivirus y manténgalos siempre actualizados.
b. No seguir enlaces no solicitados y que desconozca o dude.
c. Extremar el cuidado a la hora de descargar e instalar aplicaciones.
d. Es muy importante tener el *software* de nuestros equipos actualizados, en particular en lo que a materia de seguridad se refiere (Sistema Operativo, Navegadores, Antivirus, *AntiSpyware*, etc.) y sobre todo actualizados directamente desde el sitio *web* del proveedor.

e. Y como siempre, intentar mantenerse informado y al día de las recomendaciones y problemas de seguridad existentes, en particular referente a la ingeniería social, y no sólo de organismos gubernamentales sino también por el gran número de foros y artículos de actualidad que nos encontramos en *Internet* y demuestran la preocupación y el cariz que está alcanzado el problema [17].

Es por tanto recomendable estar siempre al día, tanto en el *software* de nuestros ordenadores como de las recomendaciones y advertencias de seguridad. En definitiva y creo que el punto más importante, si cabe, menos técnico, es la seguridad centrada en el usuario como eslabón fundamental para garantizar la seguridad en la red. Es decir, aunque técnicamente podamos abordar y resolver todos los requisitos para garantizar la seguridad, será finalmente el usuario quien tenga en sus manos la seguridad de sus acciones.

Finalmente, otra de las importantes tareas que tiene pendientes los proveedores de Redes Sociales es el mantener un control más exhaustivo de la información contenida.

3.3.3. Ataques

En el apartado anterior se han nombrado algunos de los ataques que permiten a los *hackers* aprovechar las vulnerabilidades de *Internet* y en particular, lo relacionado con las Redes Sociales. En este sentido, para obtener una visión más amplia de las vulnerabilidades expuestas, este apartado se dedica a describir con detalle el funcionamiento de los ataques citados y, de este modo, tener un mayor conocimiento del problema con el fin de facilitar la manera de abordarlo y evitarlo o mitigarlo.

En general, cualquier equipo conectado a una red informática puede ser vulnerable a un ataque. Un "**ataque**" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de *software* o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Los ataques siempre se producen en *Internet*, a razón de varios ataques por minuto en cada equipo conectado. En su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el propietario sepa lo que está ocurriendo. En casos atípicos, son ejecutados por piratas informáticos.

Para bloquear estos ataques es importante estar familiarizado con los principales tipos y tomar las pautas y recomendaciones al respecto.

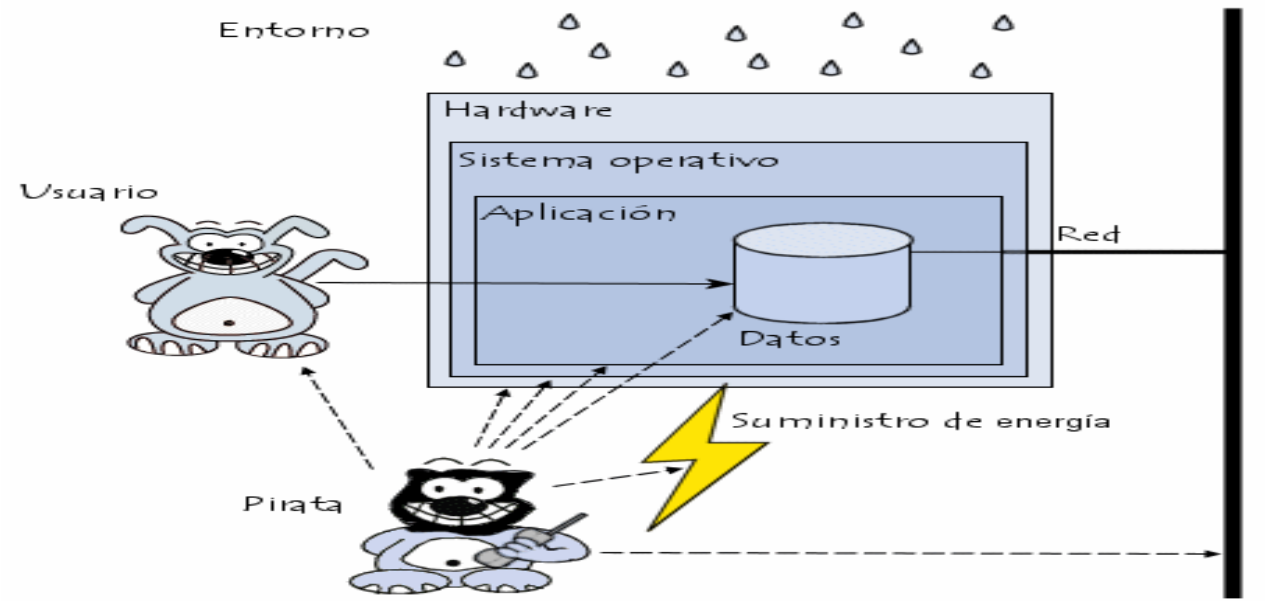
Los ataques pueden ejecutarse por diversos motivos que afectan principalmente a la privacidad de los datos de los usuarios de las Redes Sociales:

- Para recopilar información personal acerca de un determinado usuario.
- Para obtener información, como secretos industriales o propiedad intelectual al tratarse de una empresa como usuario del servicio de Red Social.
- Para obtener información de las cuentas bancarias de un usuario.
- Para obtener información acerca de una empresa.
- Para afectar el funcionamiento normal de un servicio *web*.
- Para utilizar el sistema de un usuario como un "rebote" para un ataque.
- Para usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.
- Violación de la Privacidad Locacional. La privacidad locacional es la seguridad del individuo para poder moverse libremente en el espacio público bajo circunstancias normales, sin que su posición sea grabada sistemáticamente y en secreto para un uso posterior. La publicidad de la posición en sí puede no suponer un problema, pero sí sus implicaciones.

Por tanto, es importante conocer o tipificar los tipos de ataque para poder acotar las posibles soluciones o defensas frente a ellos. Hay que tener presente que los sistemas informáticos usan una diversidad de componentes, desde electricidad para suministrar alimentación a los equipos hasta el programa de *software* ejecutado mediante el sistema operativo que usa la red.

Los ataques se pueden producir en cada eslabón de esta cadena, siempre y cuando exista una vulnerabilidad que pueda aprovecharse. El esquema que figura a continuación repasa brevemente los distintos niveles que revisten un riesgo para la seguridad:

Figura 4. Ataques: Niveles a los que se puede ver afectada la Seguridad en Internet.



Por tanto, los tipos de ataques se pueden clasificar de la siguiente manera:

- **Acceso físico:** en este caso, el atacante tiene acceso a las instalaciones e incluso a los equipos:
  - Interrupción del suministro eléctrico.
  - Apagado manual del equipo.
  - Vandalismo.
  - Apertura de la carcasa del equipo y robo del disco duro.
  - Monitoreo del tráfico de red.

- **Interceptación de las comunicaciones:**
  - Secuestro de sesión.
  - Falsificación de la identidad.
  - Redireccionamiento o alteración de mensajes.

- **Denegaciones de servicio:** el objetivo de estos ataques reside en interrumpir el funcionamiento normal de un servicio. Por lo general, las denegaciones de servicio se dividen de la siguiente manera:

- Explotación de las debilidades del protocolo TCP/IP.
- Explotación de las vulnerabilidades del *software* del servidor.

- **Intrusiones:**

- Análisis de puertos.
- Elevación de privilegios: este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). En ciertos casos, esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de desbordamiento de la memoria intermedia (búfer) usan este principio.
- Ataques malintencionados (virus, gusanos, troyanos).

- **Ingeniería social:** en la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto. Cuando ello sucede, ningún dispositivo puede proteger al usuario contra la falsificación: sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.

- **Puertas trampa:** son puertas traseras ocultas en un programa de *software* que brindan acceso su diseñador en todo momento.

Entre otros ataques también podemos citar:

- Ataques **Criptográficos:** de Contraseñas, Ataque *MitM* o Ataque de *REPLAY* entre otros.

- Ataques mediante **Denegación de Servicio:** tales como el Ataque *smurf*, Ataque *POD* (*Ping* de la muerte), Ataque por fragmentación, Ataque *LAND* o Ataque *SYN*.

- Ataques mediante **Técnicas:** tales como Suplantación de dirección IP, Secuestro de sesión TCP, Envenenamiento de ARP, Analizadores de red (rastreadores de puertos), Análisis de puertos, Desbordamiento de búfer o Bombardeo de correo electrónico.

- Ataques que aprovechan las **Vulnerabilidades** de la *web*: tales como Ataques al servidor *web*, Manipulación de datos, Manipulación de *URL* o ataques de secuencia de comandos entre sitios (XSS).

- Otros ataques que propician las **Estafas:** Fraude de transferencia de fondos (*Scam*).

Se puede ampliar y encontrar más información detallada de estos ataques en la *Wikipedia* o en numerosos artículos en *Internet*, entre los cuales, nos encontramos con la *Kioskea.ne*t [17] cuyos artículos de seguridad, recomendaciones, trucos y ataques en *Internet* son muy interesantes y prácticos.

Como hemos citado, entre los ataques que afectan particularmente a las Redes Sociales nos encontramos con:

- **Correo no deseado o *SPAM*:** El "Correo no deseado" (también se usa el término *Spam* o correo basura) se refiere al envío de correo electrónico masivo no solicitado. Conceptualmente, el término "correo no deseado" se usa para describir el envío de correos electrónicos abundantes (casi siempre de publicidad, aunque en este caso, para propagar *software* maligno) a destinatarios que no los solicitan y cuyas direcciones, por lo general, se consiguen a través de *Internet*. Funcionalmente los "*Spammers*" o las personas que envían correos electrónicos abundantes no deseados, recogen direcciones de correo electrónico de *Internet* (en foros, páginas *web*, grupos de discusión, Redes Sociales, etc.) gracias a programas de *software* llamados "*ROBOTS*ò que exploran varias páginas y almacenan en una base de datos todas las direcciones de correo electrónico que aparezcan en ellos. En este punto, el *Spammer* sólo tiene que iniciar una aplicación que envía el mensaje de publicidad o con el *software* maligno a cada dirección de manera sucesiva a la espera de que el usuario, al recibirlo, hará el resto, o no [18].
- **Suplantación de identidad o *Phishing*:** El *Phishing* (contracción de las palabras en inglés *fishing* y *phreaking*, que se refiere a piratear líneas telefónicas), es una técnica fraudulenta que usan los *hackers* para conseguir información (aunque se busca un mayor ánimo de lucro actuando sobre cuentas bancarias también nos lo encontramos en la Redes Sociales) de los usuarios de *Internet*. Dicho ataque se presenta dentro de las técnicas de "ingeniería social", lo que significa que no aprovecha una vulnerabilidad en los ordenadores sino un "fallo humano" al engañar a los usuarios de *Internet* con un correo electrónico que aparentemente proviene de una empresa fiable, comúnmente de una página *web* bancaria o corporativa. Estos *hackers* envían un correo electrónico usurpando la identidad de una empresa (un banco, una página *web* de comercio electrónico, Red Social, etc.) e invitan al usuario a conectarse a través de un vínculo de hipertexto y a llenar un formulario en una página *web* falsa, copia exacta de la original, con el pretexto de actualizar el servicio, una intervención de soporte técnico, etc. De esta forma, los *hackers* obtienen con éxito los nombres de registro y las contraseñas de los usuarios o incluso información personal que posteriormente podrá usar con motivaciones ilícitas [18].

- **Inyección *SQL*:** Los ataques de inyección *SQL* (*Structure Query Language*) atacan los sitios *web* que dependen de bases de datos relacionadas. En este tipo de páginas *web*, los parámetros se pasan a la base de datos como una consulta de *SQL*. Si un diseñador no verifica los parámetros que se pasan en la consulta de *SQL*, un *hacker* puede modificar la consulta para acceder a toda la base de datos e incluso modificar su contenido. Algunos caracteres posibilitan coordinar varias consultas de *SQL* o ignorar el resto de la consulta. Al insertar este tipo de carácter en la consulta, un *hacker* puede ejecutar potencialmente la consulta que elija. A continuación, se pueden ver algunos ejemplos:

  Ante la siguiente consulta, que espera un nombre de usuario como parámetro:

  *SELECT * FROM usuarios WHERE nombre="$nombre";*

  Un intruso sólo necesita escribir un nombre, por ejemplo, "toto" O 1=1 O nombre="titi" para que la consulta quede de la siguiente manera:

  *SELECT * FROM usuarios WHERE nombre="toto" OR 1=1 OR nombre="titi";*

  Con la consulta anterior, siempre se realiza la cláusula WHERE, lo que significa que devolverá registros que corresponden a todos los usuarios, entendemos como "código inyectado" a aquel que corresponde al código malicioso.

  Además, algunos sistemas de administración de bases de datos, como por ejemplo Microsoft SQL Server, poseen procedimientos almacenados que posibilitan ejecutar comandos de administración. Estos procedimientos son potencialmente peligrosos ya que permiten que un usuario malintencionado ejecute comandos de sistema que puedan causar una posible intrusión. Ante esta situación, existen algunas reglas que pueden ayudar a protegerse contra ataques de inyección SQL, tales como:

  - Verificar el formato de los datos de entrada y, en particular, si hay caracteres especiales.
  - No dejar que se vean mensajes de error explícitos que muestren la consulta o parte de la consulta de SQL.
  - Eliminar las cuentas de usuario que no se usen y especialmente las predeterminadas.
  - No aceptar cuentas sin contraseñas.
  - Mantener al mínimo los privilegios de las cuentas que se usan.
  - Eliminar los procedimientos almacenados.

3.3.4. Defensas

De los ataques anteriormente citados, nos encontramos con algunas defensas, de tipo técnico, que previenen y contrarrestan el ataque, singularmente para los ataques más comunes como son el *Spam*, el *Phishing* y la suplantación de la identidad. Para cada uno de estos ataques vamos a dar algunos detalles de las diferentes técnicas existentes para contrarrestarlos o prevenirlos:

- **Correo no deseado o *SPAM*:** Citaremos a continuación algunas de las diferentes técnicas o tecnologías que intentan protegernos de este ataque. Estas son:

    - Nos abrimos una cuenta en un servidor de correo *web* gratuito, por ejemplo en Yahoo (*minuevacuenta@yahoo.com*).
    - Redirigimos nuestra cuenta de correo (micorreopop@miservidor.com) hacia la cuenta de correo *web*.
    - Configuramos nuestro lector de correo (por ejemplo, el Outlook Express) para que sólo lea el correo desde la cuenta de correo *web* (*minuevacuenta@yahoo.com*). Así habremos conseguido librarnos aproximadamente del 90-95% de la basura que circula por la red. No obstante, hay que tener un par de precauciones:

        - Si dejamos nuestro buzón original (micorreopop@miservidor.com) como tal, es posible que en poco tiempo se nos llene con todo el *Spam* recibido y deje de redireccionar los mensajes. Por eso es importante utilizar una cuenta sólo redirigida.
        - Si queremos enviar correo necesitaremos una segunda cuenta que sí envíe y reciba pero hay que ser muy cauto con ella y no dársela a nadie ni publicarla en foros y otros sitios *web* de acceso público porque si no, será finalmente objetivo del *Spam* antes de que nos demos cuenta.

Otra técnica es evitar que los "*ROBOTS*ò realicen copias masivas de direcciones de correo localizadas en las páginas *web*, como por ejemplo resuelve la *web* de la facultad u otras *web*s, inhabilitando el acceso a los contenidos de las páginas (normalmente con *Javascript*) o poniendo imágenes que representan los *emails* en vez de formato texto. Esto no impide absolutamente que se copien pero sí que dificulta la tarea y obliga a realizar programas "*ROBOTS*ò más sofisticados. Si cabe indicar que, toda cura tiene su enfermedad y se pueden encontrar en las referencias ejemplos para romper estas protecciones [20].

Por último, otra técnica para protegernos de este ataque, se basa en el uso de CAPTCHAS (*Completely Automated Public Turing test to tell Computers and Humans Apart*) o prueba de Turing pública y automática para diferenciar a máquinas y humanos, los cuales son utilizados para evitar que robots, también llamados *Spambots*, puedan utilizar ciertos servicios. Por ejemplo, para que no puedan participar en encuestas, registrarse para usar cuentas de correo electrónico (o su uso para envío de correo basura) o, más recientemente, para evitar que correo basura pueda ser enviado por un robot (el remitente debe pasar el *test* antes de que se entregue al destinatario). Además indicar que existen innumerables implementaciones de *CAPTCHAS* e incluso servicios gratuitos [20].

- ***Phishing*:** Citaremos a continuación algunas de las diferentes tecnologías que intentan protegernos de este ataque. Estas son:

    - Protocolos seguros SSL: En general, la tecnología estándar SSL (*Secure Socket Layer*) establece la encriptación de datos y proporciona privacidad a la información que se transmite entre dos puntos, permitiendo que sólo sea conocida por su origen (el usuario) y el destino (el dominio, p.e. un banco) evitando así los riesgos de intrusión por parte de personas no autorizadas. Esto se logra empleando una llave pública para la encriptación, en donde el servidor será el único capaz de desencriptar la información con una llave secreta. Todo este proceso es realizado de manera transparente para el cliente, el cual puede verificar si su información está siendo encriptada. Para verificarlo, basta con observar que la dirección *web* introducida en la barra del navegador identifica el uso de un protocolo seguro (empieza por ñ*https://*ò) y observando además en dicha barra del navegador el candado que está ubicado en la parte inferior derecha de la ventana de su navegador es visualizado como cerrado confirmando que la página es segura. Sin embargo, señalar que no nos previene completamente ante el *phising* ya que un certificado firmado SSL por una Autoridad Certificadora sólo asegura que la información que pasa de un extremo a otro (usuario y dominio) está cifrada pero SSL no puede indicarnos si el sitio es ñrealò o no. Una configuración útil sería indicar a nuestro navegador que nos avise mediante una alarma emergente si estamos ingresando en una página segura o saliendo de ella configurándolo a través de de la opción: ñHerramientas > Opciones de *Internet* > Opciones Avanzadas > Seguridad > Advertir del cambio entre modalidad segura y no segura.ò, para el caso de *Internet* Explorer.
    - Validación Ampliada EV-SSL: Como hemos visto anteriormente, SSL no nos asegura que el sitio al cual nos conectamos es realmente quien dice ser y, en este sentido, observamos que la clave para revertir la situación de los delitos informáticos es convertir a la *Internet* en un

entorno menos permisivo para los criminales, distinguiendo las partes de la red cuya confiabilidad esté asegurada para el usuario. Aquí es donde los Certificados EV-SSL (*Extended Validation SSL*) de Validación Ampliada se presentan como una de las herramientas que se han introducido para permitir que los clientes puedan identificar los sitios *web* verdaderos. Estos certificados le brindan al usuario un indicio mucho más visible (e informativo) de que la conexión al sitio es segura. La manera de mostrarlo en IE7 y *Firefox* 3 (o superior) es muy común, en ambos casos, la barra de direcciones se pone verde de manera que autentifica y da como válida la autenticidad de ese portal al cual nos estamos conectando. Hasta ahora, los Certificados EV-SSL de Validación Ampliada han tenido un efecto mucho mayor del esperado sobre la conducta de los usuarios. Los comerciantes de *Internet* que han implementado los Certificados EV-SSL han informado que el número de carritos de compras abandonados ha disminuido en un 8,6%, y algunos comerciantes han reportado un incremento del 13% al 27% en las ventas. Por ejemplo, *Paypal*, vetará la entrada al navegador Safari porque considera inseguros todos aquellos navegadores que no incluyan el certificado *Extended Validation SSL Certificates*. El proceso de obtención de este tipo de certificados puede consultarse, por ejemplo en *GlobalSign GMO Internet Group* [21].

- *Software* de seguridad que se instala en el equipo del usuario: Como por ejemplo, *Mcafee*, que proporciona en sus productos utilidades o herramientas *anti-Phishing*, las cuales previenen y contrarrestan los ataques de una manera muy efectiva. Consultando la documentación que proporciona, encontramos más detalles en sus *whitepapers*, en particular *McAfee Research Anti-Phishing: Best Practices for Institutions and Consumers* [22] donde describe las diferentes estrategias técnicas que utiliza su *software* para protegernos de dichos ataques (entre otros, como el *Spam*) y que, en general, se pueden extender a los diferentes productos que nos encontramos en el mercado que cubren estas necesidades de seguridad. La siguiente figura ilustra el modelo básico de actividades que realiza para proteger nuestro ordenador de estos ataques:

Figura 5. Mcafee Anti-Phishing: Tres métodos de defensa ante un ataque [REF_FIG5].

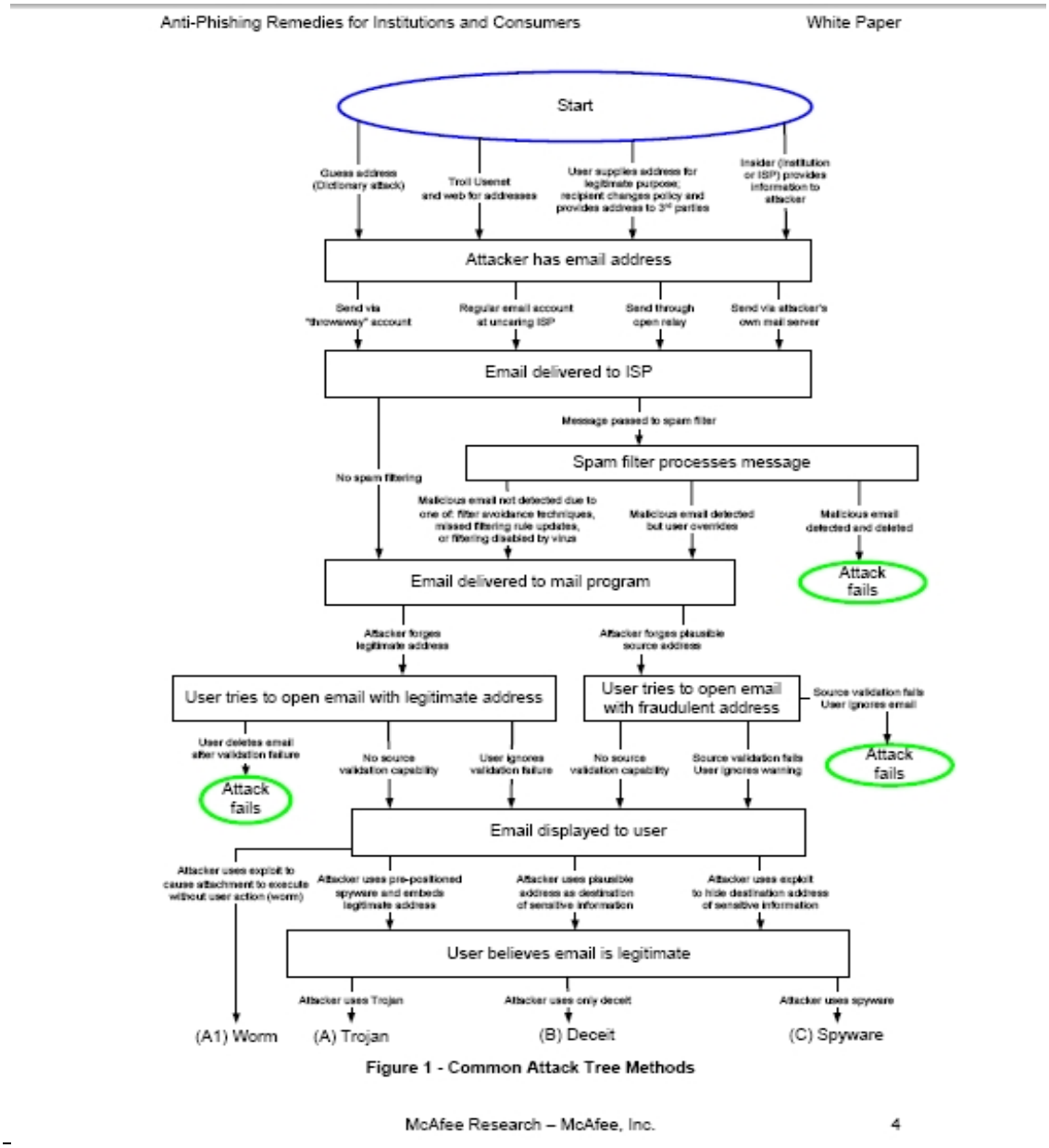


Figure 1 - Common Attack Tree Methods

McAfee Research – McAfee, Inc. 4

- **Suplantación de identidad:** Particularmente el problema parte de la carencia de una identificación robusta y que, en este sentido, dentro del ámbito de las Redes Sociales, se están incorporando diferentes estrategias, como se ha citado anteriormente, para cubrir el problema de la identificación y la autenticación, como el prometedor *OpenID* con el desarrollo de un sistema blando de identidad,

u *OAuth* para la autenticación entre los usuarios de las Redes Sociales y servicios de terceros, o los denominados sistemas de doble autenticación (o de doble factor) por *software* o la doble autenticación física basada en tarjetas de coordenadas o mediante *Tokens*, generalmente más robustos que los sistemas *software*. Es por tanto palpable el compromiso y la evolución en esta materia de seguridad pero siempre tienen presente que su incorporación no penalice el servicio, su viabilidad, su uso, y sobre todo, los costes. Uno de los principales problemas de seguridad de hoy día, es el robo de identidad. En su aspecto más popular, el *Phishing*, se ha convertido en una amenaza relevante para el canal electrónico ya sea en banca, comercio electrónico o incluso el caso de estudio, las Redes Sociales. Los mecanismos existentes para la identificación digital basados en clave de acceso, donde su fiabilidad se basa en la ñrobustezò de la política de contraseñas, no ofrecen las suficientes garantías para prevenir el problema y, por tanto, se requieren otros sistemas más sofisticados, teniendo siempre presente su viabilidad en este contexto, aquellos que están basados en *Tokens*, como mecanismo que ofrece una autenticación robusta, que permiten, entre otras características, el almacenamiento de valores de autenticación genéricos o configurarse específicamente para soporte PKI (certificados en formato PKCS12 con clave privada+pública que soportan *login* automático, certificados de usuario X509, etc.). Otros sistemas como *SmartCard*, más sofisticados y robustos, al requerir un hardware específico, disparan los costes haciendo inviable la solución, al igual que ocurre con los sistemas biométricos, y sin embargo, al contrario de los *Tokens*, que para el tipo físico, usan un hardware-*software* estándar como el USB. Los mecanismos de autenticación robusta, son una respuesta efectiva a este problema, pero hasta hace algún tiempo, su coste, debido al uso de un *Token* de *hardware* era prohibitivo para el uso masivo. Actualmente existen soluciones mediante *software*, que ofrecen características suficientes de seguridad y un coste abordable para obtener una autenticación robusta en estos nuevos escenarios. Normalmente las nuevas tecnologías abordables que proponen una solución de autenticación robusta incorporan un segundo factor de autenticación adicional, además de nombre de usuario y clave, denominado doble autenticación o doble factor. Normalmente, si estamos en el caso de una doble autenticación física, - la doble autenticación por *software* (como el presentado por la empresa Arcot para *Google Apps Premier Edition* denominado *Arcot A-OK On-Demand*) -, cada usuario recibe una tarjeta con una matriz de coordenadas. La matriz es única para cada usuario, y es generada aleatoriamente. Para autentificarse, el usuario empleará su método de autentificación tradicional y recibirá un requerimiento aleatorio (desafío) que será utilizado para demostrar que está en posesión de su segundo factor de autentificación. El desafío corresponde a un conjunto de coordenadas (A2, C4, etc.) las que deben ser localizadas en la tarjeta.

Otra solución que solventaría el problema de raíz es extender el uso del DNIe (DNI electrónico), el DNIe contiene un certificado específico para realizar funciones de autenticación. Gracias a este certificado, se proporciona la garantía de la autenticidad en el origen. Con el DNIe uno puede acreditar su identidad de forma electrónica frente a terceros, además de servir como identificación física, como el antiguo. Lo más novedoso y destacado es que hace posible realizar acciones electrónicas con plena validez legal, ya que identifica al propietario como persona.

El certificado de firma que contiene el DNIe, se proporcionan estas dos garantías, además de la de autenticidad de origen:

- **No repudio de origen**: Asegura que el documento proviene del ciudadano de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del Certificado de Firma. El receptor de un mensaje, firmado electrónicamente, puede verificar la validez del certificado empleado para esa firma, utilizando cualquiera de las Autoridades de Validación del DNIe. Dado que el DNIe es un dispositivo seguro de creación de firma y que las claves de firma permanecen desde el momento de su creación bajo el control del ciudadano titular, se garantiza el compromiso del mismo con la firma realizada (garantía de "no repudio").

- **Integridad**: Con el empleo del Certificado de Firma, se puede comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones, que se utilizan siempre que se realiza una firma electrónica. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de su resumen.

Existen otras opciones menos eficaces de doble factor de autenticación, que incluye dispositivos de hardware autónomos, como los *Tokens* [23] de contraseña de un solo uso (*One Time Password*, OTP) donde se proporciona una infraestructura de autenticación unificada (ejemplos como *Unified Authentication* de *VeriSign* proponen este método de doble factor como alternativa) y se presenta como un sistema de autenticación previo a la validación de red que posibilita el acceso a los servicios corporativos, utilizando una contraseña de validez limitada; es decir, de un sólo uso. En cualquier caso, los usos típicos de *OTP* los encontramos en *OWA* (*Outlook web Access*), VPN/RAS2, Citrix3, etc.

Se pone de manifiesto que con sistemas de doble autenticación se consigue una autenticación robusta al utilizar dos factores (clave y desafío), presentando un nivel de robustez superior al de la opción clásica de clave y nombre de usuario (si alguien conoce la clave, no es suficiente para autenticarse, y si accede a la tarjeta, requiere además la clave), y sin comprometer la relación coste-efectividad al estar basada en un principio tan simple como una tarjeta plástica, cuya solución puede ser extendida a toda la base instalada de usuarios, con un coste menor a otras alternativas. Otro factor importante es la sencillez de uso de esta tecnología además de ser cómoda en cuanto al transporte y de fácil protección. Además, algunas implementaciones para algunos sistemas específicos pueden incorporar lo que se denomina una ñ**Autenticación Mutua**ò como un mecanismo complementario que permite que tal como el sitio *web* autentica al usuario, el usuario pueda autenticar al sitio *web*, el que le presenta algún tipo de información familiar y conocida por él (por ejemplo, una foto de una mascota por ejemplo).

Aun así, estos mecanismos basados en *Tokens* presentan algunos problemas que no hay que perder de vista, tales como:

- No prueba quien es la persona que tiene el *Token*.
- No autorizan a los individuos, sino a los *Tokens*.
- Si se extravía otra persona podría llegar a utilizarla y la persona ñlegalò no puede acceder al servicio prestado.
- En ocasiones pueden ser falsificadas.

Se presentan como soluciones intermedias válidas que proporcionan la identificación y autenticación robusta necesaria para cubrir los nuevos restos de seguridad que proponen las Redes Sociales.

3.4. Tratamiento de menores

Si bien es cierto que los sitios *web* de Redes Sociales pueden ampliar tu círculo de amigos, también pueden ampliar tu exposición a otras personas con intenciones poco amigables, en particular, dicha vulnerabilidad se acentúa en los menores y discapacitados físicos y psíquicos, los cuales su presencia está creciendo en este tipo de plataformas y sobre todo, las lagunas legales que esto conlleva**.**

Llama la atención la inexistencia en las Redes Sociales de sistemas eficaces para identificar y verificar la edad de los usuarios, y que controlen y limiten el acceso de menores de edad, tal y como exige la legislación actual, y sobre todo, el desconocimiento de un consentimiento válido por parte de un adulto.

Destacar la importancia del tratamiento de la seguridad en cuanto a los menores y adolescentes debido al incremento en alza de este tipo de perfil de usuarios en las Redes Sociales como demuestra la siguiente tabla que desprende el estudio Observatorio de Evolución de las Redes Sociales [24]:

Figura 6. Representación de las Redes Sociales por edades.

La principal problemática en la actualidad es el denominado *Child Grooming [25]* de niños por internet y en concreto en las Redes Sociales. Consistente en acciones por parte de un adulto para establecer vínculos de amistad con un niño a través de las Redes Sociales, con la finalidad de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual a través de medios de abusos al menor que pueden durar semanas o incluso meses (*Ciberbullyng*) [26].

Una gran ventaja del *Ciberbullying y el Child Grooming* para los acosadores es su **anonimato digital**. Por tanto pueden sentir menos sentimiento de culpa, e incluso no ser conscientes de las consecuencias de sus actos. Asimismo, tendrán menos probabilidades de ser perseguidos por la justicia, puesto que actúan desde perfiles falsos que posteriormente eliminan sin dejar ningún tipo de pista en la red. De este modo el acoso ya no se limitará necesariamente a alumnos conflictivos con malas relaciones con

los profesores, sino que también podría tratarse de alumnos brillantes sin miedo a tener mala fama. Además, como consecuencia del anonimato digital, los acosadores ya no tienen que ser físicamente más fuerte que sus víctimas, o que estar amparados por un gran número de personas.

El aumento de usuarios menores y de los *problemas* mencionados anteriormente en estas redes es la consecuencia del creciente interés por la seguridad de los mismos, y porque además cada vez más son los casos y problemas de inseguridad detectados.

En este sentido, las principales Redes Sociales conscientes del problema, están abordando las diferentes estrategias para cubrir las actuales carencias que se presentan en cuanto a seguridad y vemos que se están realizando esfuerzos para proteger al menor, eso sí, teniendo siempre presente la viabilidad y el coste-efectividad que producen las nuevas mejoras en la red. Y por supuesto, bajo la atenta mirada de los correspondientes organismos oficiales encargados de velar y regular la seguridad en *Internet*.

En la actualidad, uno de los principales problemas de estas redes es la carencia de un sistema de autenticación robusto. La principal consecuencia que desprende es que no existe una manera completamente factible para controlar la edad del menor y por tanto, la dificultad para aplicar las directivas apropiadas en pos de su protección, entre las posibles situaciones que se pueden encontrar, el usuario, aunque reciba los mensajes pertinentes de avisos en cuanto al control del menor y demás, en última instancia, puede mentir, y de hecho así sucede en la mayoría de los casos.

Aunque es cierto que se pueden encontrar artículos y alguna noticia de nuevas tecnologías basadas en una "tecnología del comportamiento" [27] para intentar asegurar que la gente tiene la edad que dice tener en la Red Social y así eliminar del sistema a la gente que engaña. Dicha tecnología podría identificar, por ejemplo, cuando alguien se hace amigo de gente de edades significativamente dispares, un indicio de que algo está mal.

Otras serían, como se indica más adelante en el documento, mediante algún tipo de certificación de la identidad, como por ejemplo, *OpenID* y el desarrollo de un nuevo sistema blando de identidad [19]. Otros ejemplos de mecanismos de identificación en los que se está trabajando, - algunos ya disponibles -, son los denominados sistemas de doble autenticación (como el presentado por la empresa *Arcot* para *Google Apps Premier Edition* denominado *Arcot A-OK On-Demand*) donde, en este caso, la doble autenticación no se realizará ni con tarjetas, ni *Tokens* ni con ningún otro tipo de hardware, sino mediante un fichero cifrado alojado en el ordenador del propietario/usuario, el que realiza el doble factor,

donde su presencia autentica al usuario en segunda instancia, siendo el factor primario de autenticación el conocido uso de usuario y contraseña.

Desde el punto de vista de la seguridad, parece que los dobles factores son interesantes y por tanto elogiables, aunque el hecho de tener cosas instaladas en el equipo (ficheros cifrados, *cookies*, etcé) es susceptible de ser atacado y por tanto, es preferible la doble autenticación física, como las tarjetas de coordenadas o los *tokens*, que generalmente son más robustos que los métodos *software*.

De todos los sistemas que se van presentando referentes a las llamadas tecnologías de verificación de edad, las cuales intentan autentificar la identidad y edad de los niños y evitar que los adultos los contacten, se llega a la conclusión que, por el momento, no ofrecen las garantías necesarias para proteger al menor porque no garantiza completamente la verificación de la edad del mismo, en contraste con los adultos, con los cuales sí ocurre en mayor medida, entre otras razones, porque la dificultad de verificar la edad e identidad de los niños es que éstos no cuentan con licencia de conducir o del seguro social o de algún título acreditativo oficial como ocurre con los adultos.

Tecnológicamente hablando, las líneas o directrices que describen la piedra angular de la seguridad de los menores en las Redes Sociales, y que proponen los organismos de seguridad como la AEPD (Agencia Española de Protección de Datos) o, en Estados Unidos, la ISTTF, se pueden agrupar en las siguientes categorías, de las cuales ya existen aportaciones técnicas por parte de las Redes Sociales según describe el último informe de ISTTF (*Internet Safety Technical Task Force*) *Enhancing Child Safety & Online Technologies* [29]:

- **Verificación de la Edad, Identificación y Autenticación del menor** donde, además de lo citado hasta el momento, ofrecen otras soluciones técnicas como la posibilidad de creación de bases de datos públicas sobre el estado de los individuos (hechos delictivos, etc.) o bases de datos generadas por entidades públicas como colegios, donde se podría tener un registro de los menores para su control u otras entidades como *CheckMyage.com* que permite a los padres o tutores registrar a sus hijos para acceder a un *Internet* más seguro); o los denominados ñ*peer-based verification*ò donde el resto de la comunidad evalúa mediante votaciones o recomendaciones, si una persona está en el grupo de relación apropiado con respecto a su edad. Finalmente, soluciones de identificación mediante biometría aunque estas últimas presentan los inconvenientes típicos que hacen que una tecnología no vea la luz en un sector concreto, su coste y su dificultad de implantación entre otros.

- **Filtrado, Monitorización y Auditoria** de la interacción y contenidos del espacio para prevenir, en general, el acceso a contenido inapropiado o en su defecto, monitorizar su actividad. Dichas acciones se realizan tanto en el lado cliente (*software* instalado en el equipo del usuario) como en el servidor donde dicho *software* sólo es efectivo si se combina con la supervisión, en particular la de los padres o tutores (en el lado del usuario).
- **Análisis de Textos** como tecnologías que automáticamente, supervisan y analizan el contenido del espacio, en particular las conversaciones mantenidas en la red y donde la tecnología proporciona una mejora importante en pos de la seguridad del menor. Estas tecnologías normalmente se complementan particularmente con las propuestas en la categoría anterior. No hay que olvidar que nos encontramos con ciertas incompatibilidades en cuanto a los derechos de la privacidad y seguridad se refiere.
- **Tecnologías Biométricas** donde nos encontramos soluciones de identificación individual mediante huella digital, iris o ADN entre otras ya disponibles pero con limitaciones en cuanto al coste y dificultad de implantación.
- **Otras como la Identificación Individual** donde define un registro individual de las personas convictas o con expedientes delictivos, en particular delitos que afectan a los menores donde nos encontramos la problemática de la necesidad de un sistema robusto por la criticidad y privacidad de la información contenida.

Se pueden encontrar más detalles y la enumeración de las soluciones técnicas aportadas por las diferentes Redes Sociales (*Facebook*, *MySpace*, *Orkut*, etc) que intentan cubrir las categorías expuestas en el informe citado, en el Apéndice D: *Technology Advisory Board Report*. Algunas de estas, según algunas Redes Sociales, son:

- ***Facebook*:** Enfoca sus esfuerzos en la privacidad de los perfiles de sus usuarios y la manera de compartirlos incluyendo, entre otras facetas, diversos controles que permiten a los usuarios tener un mayor control de su información así como el control de la interacción entre usuarios. También incluye la tecnología de *ñpeer-verificationò* para los usuarios menores de 18, y también para estos, la definición de los perfiles con el mayor nivel de privacidad por defecto. También se incluyen el uso de *cookies* para evitar la suplantación de la identidad, o la no posibilidad de registrarse como menores de 13 años. También dispone de diferentes ñlistas negrasò para direcciones *web*, palabras o cuentas falsas que bloquean automáticamente la interacción cuando aparecen.
- ***Orkut:*** Enfoca sus esfuerzos en la identificación y borrado de contenido ilegal (tecnologías de escaneo de imágenes, detección de *Spam* o contenidos en conversaciones),

incorporación de mecanismos a los usuarios para poder detectar y prevenir el abuso y la cooperación (como por ejemplo, un enlace con ñ*Report Abuse*ò en cada página presentada en la red) y herramientas de control de contenidos exclusivas para el control y mejora de la seguridad dentro de un marco legal.

- ***MySpace:*** Enfoca sus esfuerzos en lo que denominan las ñ3 Cêsò

    1. Contenido: prevenir el acceso a contenido inapropiado, en particular, los menores
    2. Contacto: prevenir contactos no deseados
    3. Colaboración: con el resto de los actores que tienen como objetivo la seguridad en la red, en particular, los menores.

Dichas mejoras son entre otras,- muchas comunes al resto de las redes -, como la revisión de las imágenes y videos subidas a la red, endurecimiento de los límites de edad, definición de la seguridad del perfil del usuario (visibilidad y acceso), enlaces accesibles para los usuarios para mejorar la red o identificar abusos (ñ*Contact MySpace*ò o ñ*Report Abuse*ò) y no sólo desde el perfil del usuario sino también en el resto de los contenidos, tales como la mensajería, foros, imágenes y videos entre otros; también la verificación de correos, control de las aplicaciones de terceros, publicidad y recursos para los padres (tanto *software* como una *hotline* y *email* de contacto), y tecnologías propiamente de seguridad como control de *Spam*, *CAPTCHAs*, bloqueo de *phising*, *MSPLINK* (control de las referencias *web* entre la Red Social y otras *webs*) y *tracking* o traceo de usuarios entre otros.

*Tuenti e*nfoca sus esfuerzos en la implantación de sistemas efectivos para la verificación de la edad y depurar los perfiles de menores de 14 años (compromiso con la AEPD como obligatoriedad legal) así como el establecimiento por defecto del máximo grado de privacidad para los menores, no permitir indexación por los buscadores y una mejora continua en la política informativa ofrecida a los usuarios, más clara y comprensible. También hace hincapié en las políticas de privacidad como la cesión de contenidos, el tratamiento de la información de los usuarios con fines publicitarios y la eliminación del rastro de un usuario (su perfil) en el momento que un usuario se da de baja del sistema.

Recordar que, como acertadamente describe en las conclusiones del informe ñ*Technology can play a role but cannot be the sole input to improved safety for minors online*ò donde la solución se debe presentar como la combinación de todos los frentes propuestos, en particular, la combinación de todas estas tecnologías actuales y futuras.

En general, organismos como La AEPD, ENISA y la ISTTF entre otros, regulan, definen las directrices y aplican la obligatoriedad de la necesidad de "mejorar" tanto la política informativa como las políticas y

mecanismos de seguridad. Por su parte las Redes Sociales son conscientes de ello y por eso, están trabajando en esta línea, tangible en los diferentes acuerdos establecidos y continua mejora de sus sistemas.

3.5. La integración de las Redes Sociales en otras aplicaciones

Una de las principales funcionalidades en auge actualmente en las Redes Sociales, es la de permitir que en las *webs* o dispositivos (teléfonos móvil, consolas, etc.) el usuario pueda identificarse con los propios datos de la Red Social a la que pertenece. De esta manera se consigue evitar el rechazo de los usuarios a registrarse y se pueden programar funcionalidades sociales como comentarios, valoraciones, *chats*, etc., integrando completamente la información del perfil y la de sus contactos dando también mayor agilidad de navegación (en definitiva trasladas tu Red Social a esa página *web* o dispositivo).

Figura 7. Redes Sociales integradas en distintos dispositivos.

Esta integración nos proporciona:

- Apertura de nuevos canales de comunicación con los usuarios.
- Nuevas posibilidades técnicas de compartir con la comunidad distintos soportes de información.

La mayoría de esta funcionales como ***connect*** de *Facebook*, *sign in with* de *Twitter*, etc. cuando estás conectado a un sitio *web*, éste puede acceder a la información que has agregado por medio de una Red Social para permitir que interactúes con tus amigos de una forma innovadora e interesante. Las condiciones de servicio para desarrolladores de la plataforma restringen el acceso de los sitios a esta

información, y los sitios están obligados por contrato a respetar la configuración de privacidad elegida para tu cuenta. Se trata de las mismas condiciones que las que deben respetar los desarrolladores que han creado aplicaciones que usas en la Red Social, luego la seguridad en los otros sitios *web* o dispositivos en los que esté integrada la Red Social está ligada única y exclusivamente a la seguridad utilizada en la propia Red Social en un principio.

Todo esto conlleva a que si has bloqueado a un usuario en una determinada Red Social, ese usuario no podrá verte en ninguna otra página *web* o dispositivo. Cuando otros usuarios se conecten a un sitio *web*, no podrán ver ninguna información agregada por ti mediante la Red Social que no puedan encontrar navegando simplemente por la de la propia Red Social.

Para las empresas el uso de las Redes Sociales a través de teléfonos móviles está siendo uno de los principales riesgos para la seguridad de la información. Debido al gran auge del C*loud Computing* [28] es necesario contar con una estrategia sólida de seguridad. Para conocer el alcance y uso de estas estrategias en las empresas, *PriceWaterhouseCoopers*, en colaboración con *CIO Magazine* y *CSO Magazine*, ha elaborado la Encuesta Global de la Seguridad de la Información 2012, que recoge y analiza las respuestas de casi 10.000 ejecutivos y responsables de seguridad de la información y TI en todo el mundo.

Las conclusiones principales que se deducen de este estudio son:

- El 54% de los encuestados coincide en que el nivel de seguridad del C*loud Computing* [28] está mejorando frente al 23% (30,2% en España) que cree que se está debilitando.
- El 57% de los entrevistados no dispone de estrategia de seguridad relativa a *Social Media* y *gadgets* móviles (en España este porcentaje asciende al 62,5%).
- Las Redes Sociales y los dispositivos móviles vuelven a estar en entredicho en cuanto a la seguridad de la información se refiere en las empresas.
- Para la mayor parte de los encuestados, el mayor riesgo asociado al uso del *Cloud Computing* [28] radica en la incertidumbre que tienen las compañías a la hora de hacer cumplir al proveedor con los protocolos y políticas de seguridad, la dificultad en la auditoría, la problemática del control de privilegios de acceso o su difícil localización geográfica.
- El 72% de los entrevistados confía que los sistemas de seguridad son efectivos.
- En España sólo el 45,7% de los encuestados prevé incrementar la inversión en seguridad de la información en los próximos doce meses.

- El control y reducción de costes y presupuestos, así como la creciente reducción de personal en las empresas por la recesión económica, están dificultando que se alcancen los objetivos de seguridad deseados por las compañías, debido a que se reducen las inversiones en seguridad y con ello puede aumentar el riesgo de fuga de datos.

Un riesgo emergente para la seguridad de la información relacionada con uso del *Cloud Computing*, que aún no ha llegado de forma masiva a las empresas, es el llamado *Advanced Persistent Threat* (ATP).

Los ATP son unos nuevos tipos de ataques organizados que tienen como objetivo prioritario los sistemas de organizaciones internacionales, fuerzas y cuerpos de seguridad o gobiernos.

Estas amenazas todavía se centran en instituciones del sector público o la política, aunque las empresas son plenamente conscientes de la necesidad de desarrollar protocolos de seguridad en esta línea. De hecho, muchos entrevistados explican que su inversión en seguridad aumenta, de forma indirecta, su protección ante los ATP [28-a].

Como vemos, las empresas son cada vez más conscientes de la necesidad de proteger su información, de invertir en sistemas de seguridad de la información.

Es preciso asegurar que los datos de los clientes estén separados de los demás y perfectamente controlados (téngase en cuenta que éstos estarán en el *cloud*, que es un entorno compartido). En segundo lugar, existe la necesidad de garantizar la seguridad al cliente: control de datos, registro de los mismos, aplicación legislativa, procedimientos de salida y recuperación de datos, etc.

En definitiva, el modelo de C*loud Computing* trae consigo un buen número de posibilidades pero también un conjunto de riesgos potenciales. Muchos de ellos, como viene siendo habitual, vinculados a la seguridad en la red. No obstante, es previsible que estas desventajas iniciales terminen por solventarse.

CAPÍTULO 4

ASPECTOS JURIDICOS

4. ASPECTOS JURÍDICOS

El criterio seleccionado para el análisis, desde un punto de vista normativo, es el de los derechos constitucionales afectados (excepto la del derecho al olvido que aún no hay nada establecido jurídicamente), abordando su examen en función del orden de enunciación que la propia Constitución Española (CE) de 1978 establece para cada uno de estos bienes, derechos y libertades de los ciudadanos:

- La protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- La protección de datos de carácter personal.
- La protección de la producción y creación literaria, artística, científica y técnica mediante los instrumentos reguladores de la propiedad Intelectual e Industrial de las Obras.
- La protección de los derechos de consumidores y usuarios.

Así, la Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, regula de manera expresa la forma en que se debe prestar el consentimiento de los menores e incapaces para que sea adecuado en relación con la protección de los derechos al honor, intimidad y propia imagen. En este sentido, se dispone que: ñEl consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civilò

El análisis en profundidad de cada derecho atiende a un planteamiento metodológico estructurado de la siguiente forma:

- Definición del derecho.
- Marco jurídico aplicable: normativa y evolución legislativa.
- Normativa internacional.
- Normativa europea.
- Normativa nacional.
- Posibles riesgos a los que puede verse sometido el derecho.
- Colectivos especialmente vulnerables: menores de edad e incapaces.
- Medidas empleadas para salvaguardar el derecho: posicionamiento de los diferentes actores que intervienen en la cadena de valor.

4.1. Ley Orgánica 1/82 de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen

El artículo 18 de la Constitución Española se dedica a la protección de distintos bienes de la personalidad, siendo su objeto garantizar una esfera de libertad individual que protege por un lado la vida privada de las personas y les otorga, de otro, facultades que permiten ejercer un control material sobre el tratamiento de su información personal. En el precepto conviven manifestaciones clásicas de los derechos de la personalidad (derechos al honor, a la intimidad personal y familiar y a la propia imagen), una esfera de protección frente a las injerencias en ámbitos específicos (inviolabilidad del domicilio y secreto de las comunicaciones), y un derecho de última generación definido por el Tribunal Constitucional como derecho fundamental a la protección de datos. Las tecnologías de la información no sólo se proyectan sobre el último derecho citado, sino que afectan también a la conformación constitucional de las dos primeras categorías.

Los derechos fundamentales establecidos por el artículo 18 CE no son absolutos, de modo que pueden ser limitados por otros bienes o derechos constitucionalmente relevantes cuando se cumplan las condiciones que define la propia Constitución, esto es, que se establezcan mediante ley (que en todo caso respetará su contenido esencial) y se den condiciones de proporcionalidad en la adopción de las medidas limitadoras que se adopten. Ello, sin perjuicio de que en caso de conflicto con otros bienes y/o derechos constitucionales deban ceder ante otros intereses dignos de protección.

Estos derechos han sido desarrollados en el ámbito civil, penal y procesal, por leyes con contenidos y objetivos muy diversos, así como por leyes de desarrollo específico y singular, -como la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal-, conformando un complejo entramado normativo. De este modo, basta con considerar los contenidos y servicios existentes en las Redes Sociales para preguntarse de qué modo estas normas se proyectarán sobre las mismas y sobre la actividad de los usuarios.

4.1.1. Definición del derecho

La definición del bien jurídico protegido en el artículo 18 CE resulta particularmente complicada, habida cuenta de su complejidad estructural y de la influencia que sobre él ejercen los usos de las tecnologías de la información y las comunicaciones. En este sentido, y por razones puramente pedagógicas,

debería decirse que el conjunto del artículo 18 se ordena a la protección de la vida privada, como manifestación de la personalidad del individuo ligada a la protección de la dignidad y libertad del ser humano [30]. Son derechos que se integran en la categoría de los derechos de la personalidad. Su titularidad -salvo excepciones- se atribuye únicamente a personas físicas, y se caracteriza por las notas de irrenunciabilidad, intransmisibilidad, imprescriptibilidad, inalienabilidad e inembargabilidad. La vida privada se manifiesta de modo individualizado a través de distintos derechos. En primer lugar, el artículo 18.1 CE establece los derechos al honor, la intimidad personal y familiar y a la propia imagen. La jurisprudencia ha subrayado que, si bien tales derechos poseen un mismo fin, deben ser considerados independientes aunque profundamente interrelacionados [31]. El nexo entre estos derechos, e incluso con la inviolabilidad del domicilio, el secreto de las comunicaciones y el derecho fundamental a la protección de datos, no es otro que el uso de la información personal. Esta realidad no conlleva que no puedan ser analizados de forma independiente.

El derecho al honor es aquel derecho a la protección de la imagen pública de una persona, de la consideración social en la que es tenido, de su nombre y su reputación, de tal forma que el resto de individuos lo respeten durante su vida. Dicha protección, como excepción a lo usual en los derechos de la personalidad, se extiende más allá del fallecimiento por medio de acciones concedidas por el Ordenamiento a sus sucesores.

El derecho a la propia imagen atribuye al individuo la capacidad de ejercer un control sobre la captación, grabación, uso y difusión de su imagen entendida como representación gráfica de la figura humana, y también de su voz. El Tribunal Constitucional cuando se ocupa del derecho a la propia imagen no sólo atiende a los aspectos más concretos y definitorios del mismo, la facultad de consentir en la captación o difusión de imágenes que reproduzcan la figura humana, sino también a la información que éstas revelan y a su directa relación con las intromisiones en la vida privada. De hecho, debe considerarse que es esta relación con la vida privada la que dota de relevancia constitucional a la protección de la imagen y, en su caso, de la voz.

El derecho a la intimidad se entendió inicialmente por doctrina y jurisprudencia como un bien ordenado a la protección de lo más interno y reservado de las personas. Posteriormente la jurisprudencia y la evolución social han definido un derecho a la intimidad de contenido amplio y textura abierta cuyas manifestaciones son múltiples. En tal sentido, la relación de la intimidad con la propia imagen, los conflictos que se dan en el caso del ejercicio del derecho a la información y de la libertad de expresión, la práctica de pruebas corporales en el ámbito penal, la protección de la salud y la investigación

genética, y la protección de la dimensión familiar han extendido la tutela de este derecho a un ámbito más amplio.

Por último cabe destacar que la tutela constitucional de la vida privada se proyecta sobre otros dos derechos:

- La inviolabilidad del domicilio. En palabras del Tribunal Constitucional ña través de este derecho no sólo es objeto de protección el espacio físico en sí mismo considerado, sino lo que en él hay de emanación de la persona y de esfera privada de ella. Interpretada en este sentido la regla de la inviolabilidad del domicilio es de contenido amplio e impone una extensa serie de garantías y de facultades, en las que se comprenden las de vedar toda clase de invasiones incluidas las que puedan realizarse sin penetración directa por medio de aparatos mecánicos, electrónicos u otros análogos.
- La protección del secreto de las comunicaciones. Este derecho protege tanto el propio hecho de la comunicación como su contenido. Así, ñel derecho puede violarse tanto por la interceptación en sentido estricto como por el simple conocimiento antijurídico de lo comunicado. El secreto del artículo 18.3 tiene un carácter formal, ñen el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación sea al ámbito de lo personal, lo íntimo o lo reservado (STC 114/1984)ò Por tanto, el secreto de las comunicaciones se proyectará sobre todos aquellos servicios de las Redes Sociales que comporten una comunicación interpersonal que excluya a terceros distintos de los interlocutores, como los basados por ejemplo en herramientas de mensajería privada.

Dar protección eficiente a estos derechos en el ámbito de las Redes Sociales y, en general en *Internet*, conlleva la necesidad de reinterpretar, adecuar y fortalecer el concepto de protección existente hasta el momento, en la medida en que las Redes Sociales fundamentan su contenido principal en el fomento de la publicación de información personal por parte de los usuarios.

4.1.2. Marco jurídico aplicable

A continuación se presenta el análisis normativo y la evolución legislativa del derecho al honor, a la intimidad personal y familiar y a la propia imagen, haciendo especial hincapié en la protección de este derecho en *Internet*.

Se analiza el ámbito internacional, comunitario o europeo y el nacional.

Normativa internacional

La protección de estos derechos no se encuentra restringida a determinados Estados, sino que son reconocidos por la mayor parte de la comunidad internacional, siendo protegidos expresamente en las constituciones y legislaciones nacionales de muchos países.

La Declaración de Derechos Humanos de 10 de diciembre de 1948 establece la primera fuente normativa respecto a los derechos objeto de este apartado, disponiendo que: ñNadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataquesò

Del mismo modo, aunque de forma específica para los menores de edad, el Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966 y el Pacto Internacional de Derechos Económicos, Sociales y Culturales de 19 de diciembre de 1966 disponen el derecho de todos los menores a contar con un grado de protección mayor, dadas sus características particulares.

Este reconocimiento normativo en favor de los menores se recoge de forma expresa en el documento aprobado por la Convención de Derechos del Niño de 20 de noviembre de 1989, donde se dispone que ñingún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación. El niño tiene derecho a la protección de la Ley contra tales injerenciasò

Normativa europea

En primer lugar, debe hacerse referencia al Convenio de Roma de 1950 (CEDH) [32] que puede citarse como el primer texto europeo que consagra la tutela de la vida privada y junto con el Convenio núm. 108 del Consejo de Europa define el contexto normativo de la protección de la privacidad en relación con las tecnologías de la información y las comunicaciones. Frente a la escasa virtualidad de otros textos Internacionales, el Convenio de 1950 ha resultado particularmente eficaz en el ámbito de la protección de los derechos humanos en aquellos estados que han aceptado ser vinculados por sus mandatos.

La importancia del Convenio para el Ordenamiento jurídico nacional deriva de su doble naturaleza como norma incorporada al Derecho español por la vía prevista del artículo 96 de la Constitución Española y

como criterio de interpretación de los derechos fundamentales a la luz de lo dispuesto por el artículo 10.2 de la Constitución. Esta doble naturaleza se deja sentir en los efectos de las sentencias emanadas del Tribunal Europeo de Derechos Humanos en aplicación del Convenio ya que, de un lado, producen efectos jurídicos en el ordenamiento interno, y de otro, han venido inspirando la labor del Tribunal Constitucional en la interpretación de los derechos fundamentales.

En el ámbito comunitario, debe tenerse en cuenta lo dispuesto en la Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000 (2000/C 364/01 Publicada en el Diario Oficial de las Comunidades Europeas el 18 de diciembre de 2000) donde se dispone que ñToda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicacionesò

De igual forma, en la Carta Europea de Derechos del Niño (Resolución del Parlamento Europeo A3-0172/92 de 8 de julio de 1992) se declara que ñTodo niño tiene derecho a no ser objeto por parte de un tercero de intrusiones injustificadas en su vida privada, en la de su familia, ni a sufrir atentados ilegales contra su honor", reconociéndose igualmente el derecho y protección de su imagen.

Normativa nacional

A nivel nacional el reconocimiento normativo del derecho al honor, a la intimidad personal y familiar y a la propia imagen se consagraba en el artículo 18.1 CE.

Posteriormente, mediante Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, el legislador español desarrolla este derecho fundamental, estableciéndose la protección específica en materia civil.

El Código Penal dispone la regulación de los delitos relacionados con la violación de los derechos al Honor, Intimidad y Propia Imagen, con independencia del medio a través del que sean cometidos.

Desde el punto de vista del secreto de las comunicaciones y el derecho fundamental a la protección de datos, a esta norma se une la publicación de la Ley 25/2007, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, en la que se dispone la obligación de los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones de conservar los datos de tráfico generados por los usuarios a través de sus dispositivos telefónicos o de conexión a *internet*, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la

correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

4.1.3. Posibles riesgos

Como se ha señalado en apartados anteriores, las Redes Sociales no quedan exentas de peligros o posibles ataques malintencionados y pueden generarse situaciones que amenacen la integridad de los derechos al honor, intimidad personal y familiar y propia imagen del usuario, así como los derechos de terceros.

El primer momento crítico se sitúa en el registro del usuario y la configuración del perfil, dado que es la fase en la que el usuario debe valorar qué información personal desea publicar, así como configurar el grado de publicidad con el que contará dicha información. Este punto es muy importante, y ha de ser tenido en cuenta por los usuarios, pues será esencial para la posterior protección de su intimidad y de la de todos los miembros de su red.

En este momento inicial de toma de datos se incide en el derecho a la intimidad personal y familiar únicamente si se solicitan datos íntimos. Por otra parte, también repercutirá si el servicio ofrece al usuario la posibilidad de adoptar decisiones sobre su entorno. Por ejemplo, si el espacio puede ser configurado como de acceso restringido o acceso público, el uso posterior podría afectar no ya en la intimidad sino también en el honor o en la propia imagen personal o de las personas a las que eventualmente el usuario haga referencia.

Así, un posible riesgo que se puede plantear es que el usuario no establezca adecuadamente su perfil de privacidad en el momento del registro, bien por desconocimiento o porque la propia red no disponga de estas opciones de configuración.

Una correcta configuración del perfil de privacidad del usuario es fundamental, puesto que, con frecuencia, ésta se encuentra activada por defecto en la plataforma en la modalidad que permite el máximo de publicidad. Por tanto, la no configuración o la configuración incorrecta de este aspecto puede afectar no sólo a los contenidos propios que hubiera publicado el usuario, sino también al resto de los usuarios con los que hubiera publicado información compartida, puesto que ésta será accesible por parte del resto de los miembros de la plataforma.

El uso habitual que se realice de la plataforma es el segundo momento en el que la intimidad y la propia imagen pueden verse vulnerados, lo que dependerá del tipo de actividades que los usuarios lleven a cabo.

Así, se puede menoscabar la protección de estos derechos con la publicación de contenidos e información íntima en la plataforma. En este sentido, y si bien es cierto que en principio cualquier usuario controla los contenidos que desea publicar, no siempre aquél valora a priori las implicaciones de la exposición de determinados contenidos. Además, el control de la información publicada en una Red Social es limitado, en la medida en que cualquier persona o contacto de la red puede publicar fotografías, vídeos y comentarios en los que aparecen imágenes o etiquetas con el nombre de otro usuario. Este último hecho, sin duda alguna, puede poner en riesgo la integridad de los derechos mencionados, así como otros que se analizarán con posterioridad.

Además, y en línea con lo anterior, cabe señalar que el grado de información, datos e imágenes publicados pueden ser excesivos y afectar a la privacidad, tanto personal como de terceros:

- Privacidad personal: a pesar de que sean los usuarios los que voluntariamente publican sus datos, los efectos sobre la privacidad pueden tener un alcance mayor al que consideran en un primer momento, ya que estas plataformas disponen de potentes herramientas de intercambio de información, la capacidad de procesamiento y el análisis de la información facilitada por los usuarios.
- Privacidad de terceros: es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada si éstos no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata.

En la gran mayoría de ocasiones, las Redes Sociales permiten a los motores de búsqueda de *Internet* indexar en sus búsquedas los perfiles de los usuarios, junto con información de contacto y de perfiles amigos, lo que puede suponer otro riesgo para la protección de la privacidad, además de dificultar el proceso de eliminación de su información en *Internet* (surgimiento del derecho al olvido del que definiremos posteriormente).

Otro riesgo que puede aparecer durante la participación en la Red Social tiene relación con la posibilidad que tienen estas plataformas de ubicar geográficamente al usuario a través de la dirección IP y conocer el dispositivo desde el que se conecta, para contextualizar los contenidos y la publicidad mostrada.

En último lugar, en el momento en que el usuario solicite la baja del servicio como ya comentamos en el apartado 3.2, la intimidad y propia imagen también pueden verse afectadas. Esto ocurre porque, a pesar de la cancelación de la cuenta, en ocasiones la información íntima del usuario pueda continuar publicada y ser accesible desde los perfiles de otros usuarios, además de indexada y almacenada en la caché de los distintos buscadores existentes en *Internet*.

4.1.4. Colectivos especialmente vulnerables. Menores y discapacitados

Desde el punto de vista normativo en materia de protección del honor, intimidad y propia imagen, se ha de tener en cuenta la regulación específica existente.

Así, la Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, regula de manera expresa la forma en que se debe prestar el consentimiento de los menores e incapaces para que sea adecuado en relación con la protección de los derechos al honor, intimidad y propia imagen. En este sentido, se dispone que: ñEl consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civilò

Por otra parte, esta Ley establece dos principios que requieren ser contrastados con la realidad de *Internet*. En primer lugar, considera su artículo 1 que la ñprotección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familiaò Además, refiriéndose a los menores, el artículo 3 fija un criterio: la posibilidad de que un menor maduro pueda consentir en aquello que afecte a su honor, intimidad y propia imagen, y que en los casos en los que el menor no disponga de capacidad suficiente para consentir, la norma dispone que ñel consentimiento habrá de otorgarse mediante escrito por su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el Juezò

Un criterio adicional es el del artículo 4 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, que además de reconocer al menor los derechos del artículo 18 CE, establece la intervención del Ministerio Fiscal en los casos de difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o

reputación, o que sea contraria a sus intereses. Asimismo, el precepto ordena a los padres o tutores y los poderes públicos respetar estos derechos y protegerlos frente a posibles ataques de terceros.

Es evidente que la realidad de las Redes Sociales desborda la regulación y obliga a una interpretación sistemática y adecuada del ordenamiento. Por una parte, los menores de 14 años cuentan con medios tecnológicos suficientes para obtener, captar y reproducir información que afecta a su honor, intimidad e imagen y la de terceros, y de hecho lo hacen. Las fotografías de menores proliferan en *Internet* en espacios propios, en páginas familiares e incluso vinculadas a actividades escolares.

Se puede destacar que los riesgos específicos para los menores de edad en esta materia están directamente relacionados con:

- El acceso a contenidos publicados de carácter inapropiado para su edad.
- La posibilidad de entablar contacto online, e incluso presencialmente, con usuarios malintencionados.
- La proliferación de información personal gráfica de los menores publicada por ellos mismos o por terceros con desconocimiento de los riesgos asociados.

En este sentido, cabe destacar que las Redes Sociales y los sitios *web* colaborativos, en la medida en que no tienen capacidad de control sobre las publicaciones que realizan los menores, ni disponen de herramientas que garanticen la identidad plena de los usuarios, provoca mayores dificultades a la hora de lograr una protección efectiva de los usuarios de la red.

Por ello, y en tanto no sean desarrolladas y debidamente implantadas las medidas que controlen la publicación de contenidos y el acceso a material no adecuado, persistirá el riesgo de que puedan ser vulnerados los derechos de los menores.

A este factor debe añadirse que la inaplicación de la Ley Orgánica 1/1982, elaborada en un momento en el que seguramente sólo se preveían los usos mercantiles de la información y la imagen del menor, y centrada en una intervención del Ministerio Fiscal, resulta a día de hoy seguramente inviable.

4.1.5. Medidas empleadas para proteger el derecho al honor, a la intimidad y a la propia imagen de los usuarios

Las Redes Sociales y las plataformas colaborativas son los principales interesados en proteger a sus usuarios respecto a la utilización no autorizada de su información. Este hecho les ha llevado a establecer los siguientes tipos de medidas:

- Métodos de denuncia ante situaciones en las que los usuarios detecten una posible vulneración de sus derechos dentro de la plataforma.
- Sistemas de denuncia internas: Las principales Redes Sociales y sitios *web* colaborativos analizados cuentan con este tipo de medidas que permiten a cualquier usuario notificar al administrador de la Red Social la publicación de una fotografía en la que se utilice su imagen sin su consentimiento así como solicitar la retirada de un determinado comentario, vídeo o imagen que atente contra su derecho a la intimidad, honor y propia imagen. Esta denuncia genera la cancelación del contenido denunciado y la notificación al usuario denunciado de su falta de autorización para publicar más contenidos respecto al usuario denunciante (ejemplo: no se le permitirá etiquetar de nuevo al usuario en fotografías). Normalmente, en el caso de que el usuario denunciado continúe publicando contenidos en los que aparezca el usuario denunciante, se procede además a la cancelación de su cuenta por parte del administrador de la Red Social.
- Autorización expresa del usuario: Está relacionada con la medida anterior. Se requiere que el usuario relacionado con un contenido mediante etiquetas, imágenes o comentarios tenga que autorizar expresamente la publicación de éste, pudiendo incluso denunciar el contenido al administrador de la plataforma. Sin embargo, este sistema está establecido mediante un *opt out*, es decir, el usuario puede eliminar a posteriori su foto. En el caso de usuarios no registrados y que sean etiquetados, puede conllevar un mayor riesgo ya que, si bien en unas plataformas no es posible etiquetarlos, en otras es suficiente con incluir una dirección de correo.

Métodos de protección técnicos y humanos:

- Procedimientos de información: Varias de las Redes Sociales analizadas cuentan con sistemas que preavisan a los usuarios cuando alojan contenidos respecto a las implicaciones que puede conllevar, tanto para sí mismos, como para los terceros implicados. Este tipo de avisos son mostrados frecuentemente cuando los usuarios alojan contenidos multimedia, como fotografías y/o vídeos.

- Vigilancia voluntaria de contenidos: Bastantes Redes Sociales analizadas cuentan con grupos de usuarios voluntarios que se ocupan de vigilar la idoneidad de los contenidos. Estos grupos vigilan tanto los contenidos publicados por los usuarios de la red, como aquellos que, aun estando enlazados desde la plataforma, se alojan físicamente fuera de esta.
- Aplicaciones *software* de identificación de la edad: Algunas Redes Sociales han implementado, con el fin de proteger a los menores, programas que detectan la edad aproximada del usuario. La técnica empleada tiene como base el testeo de las expresiones vertidas por los usuarios en sus mensajes (empleo del lenguaje, expresiones, estilo de redacción, etc.). El objetivo de la medida se centra en:

    - Detectar la presencia y participación de menores en Redes Sociales destinadas únicamente para adultos.

    - Identificar a usuarios adultos que estén intentando suplantar o contactar con usuarios menores de edad.

  Actualmente esta medida no alcanza el grado de efectividad deseado.

- Formación y concienciación de los usuarios.
- Información sobre los deberes de los usuarios: El alta en las Redes Sociales suele venir acompañada de prolijos contratos de adhesión. En ellos las obligaciones de los usuarios se diluyen en una maraña de cláusulas contractuales. Deberían adoptarse estrategias informativas específicas que obliguen a una lectura de las obligaciones de los usuarios y que se encuentren siempre disponibles.
- Elaboración y publicación de códigos éticos: La existencia de reglas éticas de actuación no es desconocida en el mundo *Internet*. Los ISP deberían definir el estándar razonable de conducta en sus entornos, más allá de la aplicación de lo dispuesto en las normas. El fomento de códigos de autorregulación de las comunidades de una Red Social puede contribuir significativamente a la formación y concienciación de los usuarios.

4.2. Real Decreto 1720/2007 de protección de datos de carácter personal

El funcionamiento de las Redes Sociales se fundamenta principalmente en la publicación, por parte de los usuarios, de información y datos personales, lo que conlleva diferentes implicaciones jurídicas.

4.2.1. Definición del derecho

Es un derecho de configuración jurisprudencial a través de un conjunto de sentencias que arrancan con la STC 254/1993 y culminan con la STC 292/2000, cuyo fundamento jurídico define un nuevo derecho fundamental dotándolo de plena autonomía respecto del derecho a la intimidad:

ñLa garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (artículo 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es el derecho a controlar el uso de los mismos datos insertos en un programa informático y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4)ù

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (artículo 81.1 CE), bien regulando su ejercicio (artículo 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto del de la intimidad radica en su distinta función, por lo que su objeto y contenido difieran.

Según el Tribunal Constitucional el objeto del derecho a la protección de datos alcanza:

ñA cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser

accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuoò

A efectos normativos, se entiende que un dato de carácter personal es ñcualquier información concerniente a personas físicas identificadas o identificablesò, lo que convierte en dato de carácter personal la mayor parte de la información sobre personas físicas, en la medida en que a través de escasos datos o informaciones sobre éstas y mediante la correcta aplicación de herramientas informáticas, es relativamente sencillo identificar a la persona concreta que se encuentra detrás de los datos de que se dispone. Entre los datos personales que en el contexto de las Redes Sociales pueden llegar a identificar a las personas, se encuentra, entre otros, la dirección IP, tal y como ha sido definida por la Agencia Española de Protección de Datos [33] y por el Grupo de Trabajo del Artículo 29 en su ñDictamen sobre el concepto de datos personalesò[34].

Dada la gran cantidad de datos personales que los usuarios publican en sus perfiles, éstos se convierten en auténticas ñidentidades digitalesò que facilitan un rápido conocimiento de datos de contacto, preferencias y hábitos del usuario. Además debe considerarse que durante la prestación de estos servicios se recopilan datos como la dirección IP, que se utilizan para segmentar la publicidad que se dirige a los distintos tipos de usuarios, así como aumentar el grado de contacto entre los usuarios registrados.

De esta forma, y teniendo en cuenta los principios básicos dispuestos en la normativa vigente, la protección de datos personales debe ser especialmente atendida por parte de todo proyecto relacionado con el mundo de las Redes Sociales y sitios *web* colaborativos, donde el funcionamiento y tratamiento de información personal es el elemento clave para su funcionamiento.

Cabe destacar también que muchas empresas recurren a auditorías LOPD por parte de compañías auditoras especializadas, que muestran el plan de acciones a seguir acorde a las directrices que marca la AEPD caso de que no se cumplan u otorgando un certificado LOPD a la empresa si cumple con todos los requerimientos que marca la LOPD [34b].

4.2.2. Marco jurídico aplicable

El marco legal en materia de protección de datos responde a la necesidad de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, evitándose así que los datos sean utilizados de forma inadecuada o fraudulenta, o sean tratados o cedidos a terceros sin consentimiento inequívoco del titular.

Normativa internacional

Actualmente existen leyes reguladoras de la protección de datos de carácter personal en, al menos, 46 Estados. Este dato, unido al hecho de que la mayor parte de las normas publicadas son recientes y ya prevén aspectos específicos derivados de la Sociedad de la Información, hacen de la protección de datos de carácter personal uno de los aspectos más y mejor tratados desde el punto de vista legislativo.

Todo ello, unido a la existencia de varias directrices realizadas por la OCDE [35] y la ONU [36] o el Marco de Privacidad de APEC [37], hacen que los principios básicos que rigen las normativas sean semejantes o aproximados en cada uno de los Estados, sin que ello suponga que se encuentren exentas de diferencias.

Normativa europea

Del mismo modo que ocurriera con el desarrollo del derecho a la vida privada, el Consejo de Europa en el Convenio núm. 108 [38] define el contexto de protección de la privacidad en relación con las tecnologías de la información y las comunicaciones. Por otra parte, las sentencias emanadas del Tribunal Europeo de Derechos Humanos producen efectos jurídicos en el ordenamiento interno y han venido inspirando la labor del Tribunal Constitucional en la interpretación de los derechos fundamentales.

El Convenio núm. 108 surgió de la necesidad de profundizar en la protección de los derechos de los individuos en relación con el uso de la informática, en especial en lo relativo a la vida privada, protegida por el artículo 8.1 del Convenio Europeo de Derechos Humanos. Además, se debía hacer compatible esta tutela jurídica con la libertad de circulación de la información, y, por último, se consideraba necesario establecer un mínimo denominador común entre las legislaciones de los futuros Estados signatarios que permitiese facilitar el flujo internacional de datos.

El Convenio estuvo precedido por dos Resoluciones del Comité de Ministros, la R (73) 22 [39] y la R 74 29 [40], referidas a la protección de datos en los sectores privado y público respectivamente, que adelantaban algunos de los principios básicos que posteriormente inspirarían la redacción del Convenio de 1981. Atendiendo al Convenio, hay que señalar que éste posee tres partes claramente diferenciadas por su Memoria explicativa: las disposiciones de Derecho sustantivo, en forma de principios básicos; las reglas especiales referentes a los flujos internacionales de datos; y unos mecanismos de auxilio mutuo y consulta de las Partes. El Convenio ha sido completado por un conjunto de Recomendaciones dirigidas a orientar las decisiones normativas nacionales en sectores específicos:

El Convenio además define aspectos básicos como el concepto de dato de carácter personal, fichero automatizado, tratamiento automatizado o la autoridad «controladora del fichero», que hoy se define como responsable.

Asimismo, el Convenio fija los principios básicos para la protección de datos, como el de calidad o el de seguridad, los derechos de acceso, rectificación y cancelación, la protección de los datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, o la fijación de procedimientos de salvaguarda.

Por otra parte la jurisprudencia del Tribunal Europeo de Derechos Humanos ha extendido la aplicación del artículo 8 CEDH con una concepción muy amplia de la vida privada y familiar que alcanza al reconocimiento del derecho a la protección de datos en los términos del Convenio núm. 108.

En el marco de la Unión Europea el artículo 8 de la Carta Europea de Derechos Fundamentales reconoce de modo específico el derecho a la protección de datos como un derecho autónomo del derecho a la vida privada, que comprende tanto el derecho a consentir, como el deber de tratar los datos lealmente y de satisfacer los derechos de los afectados y encomienda su tutela a autoridades independientes. Este principio también se recoge en el artículo 286 del Tratado de la Comunidad Europea.

La Unión Europea publicó en el año 1995 la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos datos [41], con la finalidad de que los Estados miembros armonizasen y adaptasen sus legislaciones internas en materia de protección de datos de carácter personal.

Este texto constituye un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE).

Los aspectos clave de la normativa comunitaria en materia de protección de datos son:

- El establecimiento del principio de calidad de los datos, de tal forma que los datos personales deben ser adecuados, pertinentes y no excesivos, conforme a la finalidad para la que serán tratados.
- Se impone como principio básico y esencial para el tratamiento de datos personales la existencia del consentimiento previo del titular de los datos.
- Se requiere a los Estados que establezcan la obligación de conciliar el derecho a la intimidad en el tratamiento de los datos personales con el derecho a la libertad de expresión.
- Se establecen como principios básicos de los ciudadanos los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) en relación a sus datos personales.
- Se incorpora como principio básico la garantía de confidencialidad, así como la obligación de implantar las medidas de seguridad oportunas que garanticen que el acceso a la información se encuentra limitado y controlado.
- Se enuncian los principios básicos para la creación de las Autoridades Nacionales de Protección de Datos.
- Se fijan las bases de las transferencias internacionales de datos personales.
- Se promueve la elaboración de códigos de conducta sectoriales destinados a contribuir a la correcta aplicación de las disposiciones nacionales en materia de protección de datos personales.
- Se crea el Grupo de Trabajo del Artículo 29, institución de referencia en esta materia [42].

Debe destacarse además la importante tarea desarrollada por el Tribunal de Justicia de las Comunidades cuyas sentencias han precisado distintos aspectos en esta materia [43].

Cabe resaltar que es evidente que, aunque los ciudadanos no sepan definir con precisión el alcance y naturaleza del derecho fundamental a la protección de datos, sí lo intuyen, reconocen e identifican en cuanto éste es amenazado y puesto en riesgo, y les preocupa la seguridad de los datos personales en la Red.

Por otra parte, si bien los usuarios dicen conocer la existencia de las políticas de privacidad en *Internet*, la práctica ofrece una conclusión contraria. El número de accesos a las páginas de las políticas de privacidad es bajo, prácticamente marginal. Las políticas de privacidad ocupan espacios residuales en las páginas en *Internet* y además en las que aparecen resultan ininteligibles. Por tanto, es evidente que el ciudadano desconoce el contenido real y las consecuencias de estas políticas de privacidad. En *Internet* no puede hablarse de un consentimiento basado en información fiable o confiable. Otro tanto sucede con los rastros en la navegación, las *cookies*, la indiferencia frente a estos tratamientos desaparece cuando existe una conciencia clara de riesgo.

Este estado de cosas obliga a proponer de estándares internacionales compartidos que garanticen una eficaz protección universal de los derechos de los usuarios.

Aunque no posee valor normativo, mención especial requiere la Comunicación sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) de 2 de mayo de 2007 [44] que realizó la Comisión del Parlamento Europeo, introduciendo un claro ejemplo de la protección de los derechos de protección de datos e intimidad de los usuarios, mediante herramientas tecnológicas denominadas PET.

Las ñTecnologías de protección del derecho a la intimidadò(PET) son sistemas tecnológicos destinados a reducir y, en su caso, suprimir el impacto de las nuevas tecnologías de la información sobre los derechos de protección de datos e intimidad de los usuarios, sin que ello suponga menoscabo alguno respecto a las funcionalidades de los sistemas tecnológicos. Algunos ejemplos de PET son:

- La disociación (mantenimiento anónimo) automática de los datos. Los datos deben ser almacenados en un formato que permita identificar al interesado únicamente durante el tiempo necesario para la consecución de las finalidades para las que fueron obtenidos inicialmente. Así, una vez que los usuarios no se encuentren activos, será necesario disociar los datos de aquellos.
- El uso de instrumentos de cifrado que impidan el acceso no autorizado a la información transmitida a través de *Internet*, evitando así el tratamiento no autorizado e ilícito de los datos personales publicados en *internet*.
- El uso de anuladores de *cookies*, que impiden que el sitio *web* pueda instalar en los equipos de los usuarios ficheros que, de forma automática y sin que el usuario lo conozca, recopile toda la información estadística y relativa a los accesos que el usuario lleva a cabo durante su navegación.

- La Plataforma de Preferencias de Privacidad (P3P), que permite a los usuarios analizar y comparar las políticas de privacidad de los sitios *web* que visita, otorgándole un informe sobre la adecuación de éstas a la normativa aplicable.
- Los sistemas de gestión de identidad, que permiten el control por parte de los usuarios de los datos que revelan sobre sí mismos en cada transacción, como los promovidos por el proyecto PRIME (*Privacy and Identity Management for Europe*).

Tal como se menciona en la Comunicación de la Comisión sobre el papel de la administración electrónica en el futuro de Europa, la administración electrónica debe emplear PET para generar la confianza necesaria y prestar un servicio satisfactorio.

Mención especial tiene el Sello Europeo de Privacidad (*EuroPriSe)* surgido en 2007 y que tiene como objetivo establecer un mecanismo, que tras la oportuna evaluación, permita acreditar productos y servicios relacionados con las Tecnologías de la Información que cumplan con la normativa de protección de datos a nivel nacional y europeo.

En consecuencia, la creación y puesta en funcionamiento de este Sello Europeo de Privacidad supondrá la existencia de un certificado europeo que promueve la protección del consumidor -destinatario final de los productos y servicios certificados-, los derechos civiles y la aceptación de las normas de privacidad mediante mecanismos transparente que, finalmente, desembocará en nuevas posibilidades de introducción de las Tecnologías de Protección de la Privacidad (PETs) y un incremento de las Tecnologías de la Información.

El *EuroPriSe* está dirigido:

- A productos y servicios tecnológicos cuya finalidad sea el almacenamiento de datos personales.
- A expertos jurídicos e informáticos.
- A Agencias de Protección de Datos que pueden actuar como Autoridades de Certificación.

El mecanismo de certificación que este proyecto europeo propone, se basa en dos etapas diferenciadas:

1. En primer lugar, la autoridad de certificación debe definir un procedimiento para acreditar a los expertos que quieran realizar las correspondientes evaluaciones de productos y servicios. Todos

aquellos profesionales interesados en prestar el servicio de evaluación pueden optar a dicha acreditación. Si superan el proceso de acreditación -cuyas normas y criterios serán públicos y transparentes- y la autoridad de certificación considera que tienen las necesarias cualificaciones profesionales y satisfacen una serie de requerimientos de solvencia financiera, podrán comenzar a ejercer sus funciones como evaluadores.

2. En segundo lugar, las organizaciones interesadas en obtener el sello europeo de privacidad pueden, de forma completamente voluntaria, contactar con cualquiera de los expertos acreditados para someterse a la evaluación, que deberá llevarse a cabo utilizando los estándares y procedimientos definidos durante el proyecto. Estos estándares se han realizado teniendo en cuenta la Directiva 95/46 y la Directiva 2002/58/CE, de manera que el experto pueda auditar que el producto o servicio cumplen con las Directivas citadas. Asimismo, en el caso español, también se debe verificar que dicho producto o servicio cumple con la Ley Orgánica 15/1999, de 13 de diciembre, y su Reglamento de desarrollo. Una vez finalizada la evaluación del producto o servicio por el experto, el informe del mismo es remitido a la autoridad de certificación para su revisión. La autoridad de certificación puede aprobar el mismo, pedir aclaraciones o información adicional o, si considera que la revisión no se ha realizado correctamente o que el producto o servicio no satisface los requerimientos establecidos, simplemente rechazar la concesión del sello.

Normativa Nacional

En España, la regulación sobre protección de datos de carácter personal se centra en dos normas principalmente:

- La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD).

Además existen normas sectoriales en ámbitos como la sanidad, las telecomunicaciones o las finanzas. No obstante, las siguientes normas se proyectan de modo muy particular sobre las Redes Sociales:

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE).

- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
- Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), el objeto de la norma es la de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar.

Todo tratamiento de datos de carácter personal debe atender a una serie de principios básicos:

- Calidad de los datos: es esencial que los datos personales tratados sean adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, no pudiendo usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recabados. Los datos deberán responder con veracidad a la situación actual del afectado debiendo rectificarlos si se constatan errores. Sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento, prohibiéndose la recogida de datos por medios fraudulentos, desleales o ilícitos. Por otra parte, el responsable debe conservar los datos personales mientras subsista la finalidad y cancelarlos cuando ésta cese.
- Información en la recogida de datos, el afectado será informado, en el momento en el que se recaben sus datos, del alcance del tratamiento que se va a realizar. El artículo 5 LOPD establece que ñlos interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
    - De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
    - Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
    - De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
    - De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
    - De la identidad y dirección del responsable del tratamiento o, en su caso, de su representanteò

- Datos especialmente protegidos, este principio hace referencia a datos de carácter personal que revelan la ideología, afiliación sindical, religión, creencias -caso para el que el consentimiento debe ser expreso y por escrito-, origen racial, salud y vida, sexual -para cuyo tratamiento se requiere consentimiento expreso-, y los relativos a la comisión de infracciones penales o administrativas.
- Consentimiento del afectado o manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de sus datos personales.
- Seguridad de los datos, todas las empresas, organizaciones, asociaciones e instituciones, públicas y privadas, que almacenen, traten y accedan a ficheros de datos de carácter personal, deben aplicar medidas de seguridad técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.
- Deber de secreto, este principio recoge las obligaciones de secreto, confidencialidad y custodia que incumben a aquellas personas que traten los datos y, de manera particular, a aquéllos que en el desarrollo de sus funciones accedan a ficheros que contienen datos personales.
- Comunicación de datos, es toda revelación de datos realizada a una persona distinta del afectado o interesado. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
- Acceso a los datos por cuenta de terceros, supone la prestación de un servicio al responsable del fichero por parte de una tercera empresa, denominada encargado del tratamiento, que accede a los datos del fichero para el cumplimiento de la prestación contratada, actuando en nombre, por cuenta y de acuerdo a las instrucciones establecidas por el responsable del fichero.

Antes de realizar el análisis completo respecto a la aplicación de las normas, se ha de tener en cuenta el aspecto extraterritorial de los servicios de la Sociedad de la Información.

Dado que la gran mayoría de los proveedores de este tipo de servicios operan desde fuera de la UE (principalmente desde los EE.UU.), se ha de analizar en qué medida es posible exigir a las plataformas el cumplimiento de la normativa comunitaria. En este sentido, la normativa dispone que ésta sea de aplicación en los siguientes casos:

- Cuando el tratamiento de datos se realice en España a través de un establecimiento del responsable del tratamiento.
- En el caso de que el responsable del tratamiento no se encuentre en territorio español, pero le sea de aplicación directa la normativa española mediante acuerdos internacionales.

- Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos, medios o elementos situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

Debe considerarse que en España la normativa específica respecto a los prestadores de servicios de la Sociedad de la Información, previa fundamentación jurídica y práctica, admite la posibilidad de que las autoridades de protección de datos nacionales apliquen dicha normativa a los prestadores, con independencia del lugar desde el que se opere.

Por un lado, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, establece que existen dos casos en los que se aplica a los responsables establecidos fuera de la UE/EEE: en primer lugar, cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento ubicados en territorio español y, en segundo lugar, cuando utilice medios situados en dicho territorio.

En este sentido, el Grupo de Trabajo del Artículo 29 se ha pronunciado en su ñDictamen sobre cuestiones de protección de datos en relación con buscadoresò [46]. Este dictamen contiene una serie de criterios para definir cuándo se considera que existe un establecimiento del responsable:

ñLa existencia de un establecimiento implica el ejercicio real y efectivo de actividades a través de gestiones estables. La forma jurídica del establecimiento (una oficina local, una filial con personalidad jurídica o una representación mediante terceros) no resulta determinante. Sin embargo, otro requisito consiste en que la operación de tratamiento se realice en el marco de las actividades del establecimiento. Esto significa que el establecimiento también debe desempeñar un papel importante en la operación de tratamiento concreta. Éste es claramente el caso cuando:

- Un establecimiento es responsable de las relaciones con los usuarios del buscador en una jurisdicción concreta.
- Un proveedor de buscadores establece una oficina en un Estado miembro implicada en la venta de anuncios dirigidos a los habitantes de dicho estado.
- El establecimiento de un proveedor de buscadores cumple los autos judiciales y/o solicitudes de cumplimiento de la ley por parte de las autoridades competentes de un Estado miembro en relación con los datos de los usuariosò

Por otro lado, en lo que respecta a la prestación de servicios por parte de proveedores fuera de la UE utilizando medios situados en dicho territorio, el documento recoge una serie de criterios. Tal y como

establece el documento, ñlos centros de datos situados en el territorio de un Estado miembro pueden utilizarse para el almacenamiento y el tratamiento a distancia de datos personales. Otros tipos de medios podrían ser la utilización de ordenadores personales, terminales y servidores. La utilización de *cookies* y dispositivos de *software* similares por parte de un proveedor de servicios online también puede considerarse como recurso a medios en el territorio del Estado miembroò

Asimismo, en el año 2002 el citado Grupo de Trabajo adoptó un ñDocumento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en *Internet* por sitios *web* establecidos fuera de la UEò (WP 56)ò [44]. Dada la gran complejidad de este ámbito y el dinamismo del entorno *Internet*, este documento constituye una herramienta y punto de referencia para los responsables del tratamiento en el examen de los casos que implican el tratamiento de datos de carácter personal en *Internet* por sitios *web* establecidos fuera de la Unión Europea.

De la misma manera, la LSSI-CE contempla su aplicación a ñlos prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeoò. Así, su artículo 4 dispone que a estos prestadores les serán de aplicación los artículos sobre la libre prestación de los servicios y sobre colaboración de los prestadores de servicios de intermediación para interrumpir el servicio o retirar determinados contenidos cuando lo haya declarado un órgano español competente sobre la licitud de los mismos.

Y también establece su aplicación cuando dirijan sus servicios específicamente al territorio español, siempre que ello no sea contrario a los convenios internacionales aplicables.

A los efectos de determinar si los prestadores de servicios dirigen sus servicios específicamente al territorio español, ha de atenderse a varios elementos indiciarios:

- Si disponen de la extensión de nombre de dominio .es registrada ante *Nic.es* u operan a través de nombres de dominio ñ*es.redsocial.com*ò o ñ*redsocial.com/es*ò
- Si el sitio *web* se encuentra en castellano.
- Si tiene política de privacidad específica.
- Si el sitio *web*, por su apariencia y contenido, pudiera llegar a dar a entender que se dirige al territorio de España.
- Si la publicidad realizada es de productos y servicios distribuidos desde España.
- Si el número de usuarios españoles es elevado respecto a la muestra estadística.

- Si disponen de oficinas o agentes comerciales que traten datos personales en territorio nacional.
- Si para la prestación del servicio emplean servidores alojados en España.

En este marco, la Agencia Española de Protección de Datos ha afirmado su competencia para aplicar esta normativa a prestadores de servicios establecidos fuera del Espacio Económico Europeo respecto de la prestación del servicio del correo electrónico gratuito (Expediente E/01544/2007).

4.2.3. Posibles riesgos

El consentimiento que presta el usuario es válido en el momento en que decide aceptar, la política de privacidad y condiciones de uso de la plataforma que constan en el formulario de registro. Por ello, debe estar muy atento a su contenido y consecuencias. Evidentemente, esto no consta a que resulte exigible que las políticas de privacidad deban ser transparentes, accesibles y claras. La AEPD ha insistido sobre el particular en su ñDeclaración sobre buscadoresò, así como en la ñResolución sobre correo electrónico gratuitoò

Del mismo modo, los usuarios deben valorar siempre qué tipo de datos proporcionan a la plataforma y publican en su perfil, ya que no tiene la misma trascendencia el tratamiento por parte de la plataforma de los datos de carácter personal de nivel básico (nombre, dirección, teléfono, etc.), que otra información más sensible (nivel de renta, solvencia, recibos, afiliación sindical o política, salud, vida sexual, etc.), donde el nivel de protección y concienciación por parte del usuario deberá ser mucho mayor, dado que se trata de derechos pertenecientes a la esfera más íntima de su vida.

Por ello, a pesar de que la información contenida en los perfiles de los usuarios es alimentada directamente por éstos, es necesario tener en cuenta cuáles son los principales riesgos que se pueden derivar del uso de este tipo de plataformas para la protección de los datos de carácter personal.

Como criterio general, cabe señalar que las Redes Sociales disponen de avisos legales, condiciones de uso y políticas de privacidad, aunque en ocasiones, redactadas en un lenguaje de difícil comprensión para el usuario. De esta forma, y a pesar de encontrarse recogidas en el sitio *web*, no alcanzan su finalidad última y es la de que el usuario comprenda el objeto, la finalidad y el plazo para el que son recabados y tratados sus datos personales.

Así, el primer momento crítico para la protección de datos personales se encuentra en la fase inicial de registro del usuario, cuando éste proporciona la información personal necesaria para poder operar en la Red Social. En este momento, los datos se pueden ver sometidos a varios riesgos:

- Que el tipo de datos solicitados en el formulario de registro, aunque no obligatorios, sean excesivos. En este sentido, debe tenerse en cuenta que, con frecuencia, las Redes Sociales solicitan a los nuevos usuarios datos relativos a su ideología política, orientación sexual y preferencia religiosa. Si bien es cierto que estos datos tienen carácter voluntario y todo usuario es libre de publicar el contenido que desee respecto a sí mismo, debe considerar las implicaciones que ello puede conllevar para su vida y las personas de su entorno, ya que estos datos serán visibles por todos sus contactos y, dependiendo de la configuración del perfil, por todos los usuarios de la red. Es por ello que los usuarios y los responsables de las redes deben limitar y controlar en todo momento que el grado y la trascendencia de los datos publicados no sea extrema. Debe tenerse en cuenta que el artículo 7 LOPD obliga a contar con un consentimiento expreso y por escrito en lo que se refiere a datos relativos a ideología, religión o creencias, y expreso en el ámbito de la salud, origen racial y vida sexual.
- Que el grado de publicidad del perfil de usuario sea demasiado elevado. Es en el momento inicial del registro como usuario cuando éste debe configurar debidamente el grado de publicidad de su perfil, de tal forma que determine desde el comienzo quiénes podrán tener acceso a toda la información que el usuario publique. Todas las redes analizadas muestran, activado por defecto, el mayor grado de publicidad, resultando el perfil de acceso completamente público lo que supone un grave riesgo para la seguridad de los datos personales de los usuarios, en la medida en que éstos serán accesibles por parte de cualquier usuario de la plataforma.
- Que la finalidad de los datos no esté correctamente determinada. Con frecuencia las políticas de privacidad recogidas en este tipo de plataformas, determinan las finalidades para las que se recaban y tratan los datos personales, pero de forma generalista y sin aclarar completamente para qué pueden o no tratar los datos personales, lo que supone un grave riesgo para el tratamiento de los datos de los usuarios.
- Transferencia internacional de datos. Como se ha señalado, es frecuente que este tipo de plataformas se encuentren ubicadas fuera del territorio europeo, principalmente en EE.UU., lo que supone que en el momento de registro del usuario, los datos son trasladados a los servidores y oficinas ubicados en este país. Por ello, resulta fundamental que las políticas de privacidad del proveedor garanticen un estándar adecuado de protección. Junto a este hecho

cabe la posibilidad de que las plataformas cedan sus bases de datos a terceras organizaciones, para que lleven a cabo campañas de envío de comunicaciones comerciales no autorizadas (*Spam*) o realicen otro tipo de tratamiento que goce de menor protección en el país en el que se tratan los datos. Y ello debería ser tenido en cuenta por el usuario como criterio de elección de una determinada red.

El segundo momento considerado crítico para la protección de datos personales se sitúa en la fase intermedia, es decir, en la que el usuario desarrolla su actividad en la plataforma y utiliza los servicios y herramientas que ésta le ofrece. En este momento los aspectos que pueden poner en riesgo la seguridad y protección de datos personales de los usuarios son:

- La publicación excesiva de información personal (propia o de terceros). En esta fase se mantiene el posible riesgo que conlleva la publicación excesiva de información personal por parte de los usuarios.

  Además se debe tener en cuenta que existe la posibilidad de que los usuarios publiquen también datos respecto de terceros, lo que puede suponer el tratamiento y la cesión pública de datos de personas que no han prestado el consentimiento para ello.

  La AEPD ha sancionado la captación y publicación de imágenes de terceros en plataformas colaborativas sin consentimiento de las personas afectadas (Resolución de la Agencia Española de Protección de Datos PS/00117/2008).

  De la misma forma, la AEPD ha reconocido el derecho frente al responsable del sitio *web* a cancelar los datos publicados que habían sido facilitados por terceros en entornos online (Procedimiento TD/00266/2007).

- La instalación y uso de *cookies* sin conocimiento del usuario. Con frecuencia las Redes Sociales y plataformas análogas utilizan este tipo ficheros que tienen la posibilidad de almacenar determinada información sobre el usuario y su tipo de navegación a través de un sitio *web*.

  Estos ficheros se instalan en los equipos de los usuarios, de forma que resulta posible detectar el lugar desde el que accede el usuario, el tipo de dispositivo empleado (móvil o fijo) para el acceso, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales

realizadas durante la navegación, así como el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades.

Este modo de recabar los datos funciona de forma automática, al contrario que en el caso de los formularios.

Dado que la dirección IP86 desde la que se conecta a *Internet* el usuario es considerada por la Agencia Española de Protección de Datos un dato de carácter personal, en la medida que puede asociarse a una persona identificable, se debe entender, por ende, que a través de aquélla cabe la posibilidad de obtener información relacionada con los usos y hábitos de navegación de los usuarios de las Redes Sociales, lo que proporciona una herramienta muy valiosa desde el punto de vista del *marketing* y la publicidad.

- Uso de *web beacons* [48]. Son imágenes electrónicas que permiten al sitio *web* conocer quién y qué contenido online ha sido visitado. Normalmente estas imágenes son incluidas en correos electrónicos, anuncios, etc. Dependiendo del tipo de acceso, esta información podría incluir la dirección IP de origen de la conexión, el sistema operativo empleado, el programa gestor de correo electrónico, etc. Éstas y otras informaciones obtenidas pueden utilizarse con diferentes fines, incluso como ataques al usuario (abusando de vulnerabilidades conocidas de los programas que utiliza), confirmación de direcciones electrónicas (para envío masivo de correo electrónico no deseado o para comercialización de bases de direcciones confirmadas), etc.
- Que el perfil de usuario sea indexado automáticamente por los buscadores de *Internet*. La mayor parte de las plataformas analizadas permiten que los motores de búsqueda de los principales buscadores de *Internet* puedan indexar los perfiles de los usuarios de forma pública en la red. En algunos casos dicha indexación incluye el nombre del usuario registrado, su fotografía del perfil y el nombre y fotografías del perfil de los amigos o contactos con los que cuenta en la Red Social, así como una invitación general a entrar a formar parte de la plataforma.

  Este hecho supone una amenaza para la protección de datos personales de los usuarios, en la medida en que sus datos básicos y principales contactos se exponen públicamente en la Red, accesibles por parte de cualquier usuario, pudiendo llegar a ser empleadas esas informaciones de forma descontrolada por terceros, sin que éstos queden en el "círculo cerrado" de la Red Social. Además se debe considerar que la Agencia Española de Protección de Datos ha tutelado el derecho a oponerse a la indexación del nombre o de otro tipo de datos de carácter

personal en los buscadores, ya que supone un tratamiento automatizado de datos que debe ajustarse a todas las obligaciones dispuestas en la normativa vigente (Procedimiento TD/00463/2007).

- La recepción de publicidad hiper-contextualizada. La publicidad online es el modelo de explotación comercial más utilizado actualmente por parte de las Redes Sociales. Estas pueden determinar un grado de exactitud casi absoluto respecto del tipo de productos y servicios que el usuario va a demandar gracias a la cantidad de información que tratan respecto a cada uno de sus miembros.
- La recepción de comunicaciones comerciales electrónicas no solicitadas (*Spam*). Cada vez más, las Redes Sociales están siendo empleadas por *Spammers* como fuentes para recabar información y datos personales a los que posteriormente se dirigirán comunicaciones comerciales no deseadas.
- La suplantación de identidad de los usuarios de la Red Social. El concepto de ñsuplantación de identidadò recogido como delito en la normativa penal española adopta una nueva trascendencia en el mundo online, dado que cualquier usuario puede contar en *Internet* ï y normalmente así sucede- con varias ñidentidades digitalesò Desde luego que no se trata de un comportamiento negativo, sin embargo la posibilidad de que la identidad de una persona sea registrada por otra persona ajena aumenta considerablemente.

Así, el tercer momento crítico para la protección de datos personales se sitúa en la fase en la que el usuario pretende darse de baja del servicio. En este momento, deben tenerse en cuenta los siguientes aspectos que pueden poner en riesgo la seguridad y protección de datos personales de los usuarios:

- La imposibilidad de realizar la baja efectiva del servicio. Comprobados los procesos de alta, utilización y baja en las Redes Sociales analizadas, se ha detectado como en algunos casos, a pesar de solicitar la baja del servicio conforme a las políticas de privacidad recogidas en algunas plataformas, la baja del servicio no se ha llevado a cabo de manera efectiva, manteniéndose los datos personales de los usuarios a disposición de los responsables de la Red Social. Es frecuente que el usuario que intenta darse de baja del servicio se encuentre con procedimientos complejos que nada tienen que ver con el procedimiento automatizado y electrónico de alta en la plataforma. Este hecho implica un riesgo para la seguridad y protección de datos personales de los usuarios.
- La conservación de datos y el cumplimiento del principio de calidad de los datos. Por último, cabe señalar el posible riesgo que supone el hecho de que las Redes Sociales y otros

prestadores de servicios de la Sociedad de la Información conserven los datos de tráfico generados por los usuarios en el sistema, para utilizarlos posteriormente como herramientas a través de las que sectorizar y conocer las preferencias y perfiles de los usuarios para realizar publicidad contextualizada con el medio y contenido de sus comunicaciones a través de la Red, afectando de esta forma al principio de calidad de los datos.

Aunque el caso particular de las Redes Sociales no es idéntico al de los buscadores, se puede concluir que las Redes Sociales, como servicios de la Sociedad de la Información, deben someterse a la aplicación de la normativa de protección de datos, debiendo atender a los principios básicos que rigen la norma:

- Principio de calidad de los datos: no deben conservar los datos de forma indefinida en sus servidores.
- Principio de consentimiento: no pueden tratar datos de carácter personal sin que haya mediado el consentimiento por parte del titular de los datos.
- Principio de información: deben informar de forma clara y comprensible a todos los usuarios respecto a qué van a hacer con sus datos y del derecho a disponer respecto a los mismos en cualquier momento.

4.2.4. Colectivos especialmente Vulnerables. Menores y discapacitados

Cabe señalar que desde el punto de vista normativo, tiene especial importancia la publicación del Real Decreto 1720/2007, que aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD). Hasta su aprobación, no existía en España referencia expresa al tratamiento de datos de los menores.

El reglamento introduce una importante especialidad en lo que respecta a la prestación del consentimiento por parte de estos menores, al disponer que para recabar los datos de cualquier menor de 14 años es necesario contar con el consentimiento de los padres o tutores.

La norma señala además de manera expresa que al recabar el consentimiento del menor debe utilizarse un lenguaje sencillo y fácilmente comprensible para él y que no se podrá obtener a partir de ellos información respecto a sus familiares y allegados.

El responsable que recaba y trata datos personales de menores de edad será el responsable de articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso por los padres, tutores o representantes legales.

Estas medidas normativas implican que las Redes Sociales tienen la obligación de disponer de medios tecnológicos que garanticen la identificación de la edad de los usuarios.

Sin embargo, y a pesar de la obligación dispuesta por la norma, en la medida en que los proveedores de servicios, los fabricantes y distribuidores de soluciones de seguridad y las entidades públicas no implementen sistemas efectivos, la identificación de los menores y el tratamiento de sus datos se encuentran ante un riesgo, ya que éstos podrían estar siendo tratados bajo un consentimiento no válido.

La Agencia Española de Protección de Datos ha sancionado la falta de diligencia en la comprobación de la identificación de un menor que se registró en un sitio *web* cuyos datos se utilizaron para remitirle publicidad (Procedimiento PS/00281/2007).

Por lo que respecta a posibles situaciones particulares de riesgo que pueden conllevar aspectos negativos para la seguridad y protección de datos de los menores e incapaces, como pudiera ser la publicación de información personal y familiar, surge la necesidad de avanzar en la investigación y desarrollo de medios de identificación de la edad para alcanzar una solución efectiva y que no suponga un freno para el desarrollo de la Sociedad de la Información entre los más jóvenes.

Sin embargo, no basta con soluciones tecnológicas. Como destacó el Director de la Agencia Española de Protección de Datos en su intervención ante la 30º Conferencia Internacional de Autoridades de Protección de Datos, los riesgos para los menores en i*nternet* parten en gran medida de un déficit educacional básico: desconoce cómo ejercer un verdadero control sobre su información.

La formación actual a los menores en el uso de las nuevas tecnologías, con sus riesgos y ventajas, es insuficiente. En la escuela no se aprende a controlar la información personal ni a identificar los riesgos en la Sociedad de la Información. La formación sobre protección de datos no se ha trasladado a los programas de estudio. Por ello, resulta ineludible el compromiso real y efectivo de organismos y autoridades educativas tanto de carácter internacional como nacional.

4.2.5. Medidas empleadas para proteger el derecho de protección de datos de carácter personal

Para la correcta protección de los datos personales de los usuarios es imprescindible que éstos valoren el tipo de datos que publican en su perfil. Además, consideran crucial que las organizaciones públicas y privadas realicen, desde el momento en que se produce el registro de usuario, labores de información, formación y concienciación sobre los peligros de la publicación excesiva de contenidos.

A nivel técnico, cabe señalar las siguientes acciones:

- Eliminar los datos obsoletos que pudieran existir en distintos servidores, así como el cifrado de aquéllos que estén en uso, minimizando así los daños que pudieran resultar de un ataque desde el exterior por parte de usuarios malintencionados.
- Establecer mecanismos de análisis respecto de la fortaleza de la contraseña de manera que se obligue al usuario a seleccionar una que no sea fácilmente descifrable por terceros [46].
- Disociar los datos incluidos dentro de un perfil de usuario para que, en el caso de acceso por terceros no autorizados, éstos no puedan acceder a los datos de los usuarios y emplearlos con fines malintencionados.
- Crear categorías de perfiles para controlar el volumen de datos personales que el usuario permite que resulten visibles al resto de usuarios.
- La creación de categorías de autorizaciones por ellos mismos sobre quién puede visionar sus perfiles. En este sentido cabe destacar los siguientes elementos:
    - Limitar el grado de publicidad del perfil del usuario conforme a los criterios anteriormente expuestos.
    - Limitar la indexación de los perfiles por parte de los principales buscadores de i*nternet*.
    - Limitar la visualización del perfil de manera geográfica.
    - Limitar la cantidad de datos que los usuarios pueden introducir.

Otras acciones a realizar son los métodos de denuncia:

- Medios a través de los que denunciar situaciones que afecten a sus datos personales o intimidad en la Red Social, debiendo existir un departamento en las Redes Sociales para que, de forma automatizada en una primera fase, se bloqueen dichos contenidos y, en una segunda, pasen a ser analizados caso por caso por persona físicas. Esta medida permite a los usuarios reclamar

de forma instantánea cualquier posible vulneración de la intimidad o un uso inadecuado de los datos de carácter personal del usuario.

- A la hora de recoger datos e informaciones sobre sus usuarios, las plataformas deben guiarse por el principio de moderación, de tal forma que sólo soliciten aquellos datos que realmente son relevantes para la finalidad de la plataforma.
- Es igualmente necesario destacar que algunas plataformas de servicios de *Internet* están comenzando a iniciar programas de formación y concienciación externa en instituciones escolares y centros educativos, con la finalidad de lograr que, tanto profesores como alumnos conozcan completamente todos los beneficios y riesgos que puede suponer el uso de este tipo de servicios.

4.3. Real Decreto Legislativo 1/1996. Ley de protección de los derechos de propiedad intelectual sobre los contenidos

La facilidad de reproducción y distribución de contenidos hacen de *Internet* uno de los principales medios de crecimiento para los contenidos de propiedad intelectual, al tiempo que supone uno de los principales retos en lo que respecta al control y protección de los derechos de autor, en la medida en que los contenidos se encuentran en formato digital y, por tanto, su distribución y comunicación pública es mucho más sencilla que en otro tipo de formato.

Las Redes Sociales y, en especial, las plataformas colaborativas de contenidos multimedia (*Youtube, Dalealplay.com, Myspace, Google video, Redkaraoke*, etc.), son el mejor ejemplo de las posibilidades que brindan este tipo de plataformas a los autores.

4.3.1. Definición del derecho

A la hora de analizar la protección del derecho de propiedad intelectual en las Redes Sociales e *Internet* en general, conviene tener en consideración las siguientes premisas:

- Se considera autor a la persona física o jurídica que crea una obra.
- La propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación.

- Los derechos de propiedad intelectual se componen tanto de derechos personales como de los derechos de explotación sobre la obra.
- Son consideradas obras de propiedad intelectual las obras literarias, artísticas o científicas.

La protección se dirige, por tanto, al derecho que el autor tiene sobre su creación literaria, artística o científica.

La protección comprende tanto los derechos de carácter moral como los patrimoniales, atribuyendo al autor la plena disposición y el derecho exclusivo a la explotación de sus obras.

- Derechos Morales: son derechos inherentes a la persona física y, por tanto, irrenunciables, encontrándose entre ellos la ñpaternidadòde la obra, la integridad de la misma, la decisión sobre su difusión y el reconocimiento de su autoría.
- Derechos Patrimoniales: son derechos cuantificables económicamente y que pueden ser dispuestos por los sujetos titulares (personas físicas y jurídicas). Estos derechos son los relativos a las actividades de reproducción, distribución, comunicación pública y transformación.

En este sentido, el titular es el sujeto legitimado para autorizar la reproducción, puesta a disposición o transmisión de una obra de propiedad intelectual sobre su propiedad [50], quedando limitado por las posibilidades otorgadas por el derecho de cita, los trabajos de actualidad y las reproducciones provisionales o copias privadas, entre otras.

4.3.2. Marco jurídico aplicable

La legislación en materia de propiedad intelectual tiene por objeto proteger los derechos sobre las obras artísticas, científicas o literarias de los autores y del resto de intervinientes [51].

Normativa internacional

La normativa internacional, en materia de propiedad intelectual, se encuentra en una situación claramente ventajosa respecto a otros aspectos analizados en este proyecto. Así, en el año 96 se propuso en el seno de la Organización Mundial de la Propiedad Intelectual -OMPI o WIPO- la aprobación de dos tratados para regular la materia a nivel global:

- *WIPO Copyright Treaty* (Tratado de la OMPI sobre derecho de autor), que entró en vigor el 6 de marzo de 2002. Su objeto viene definido por la protección de las obras literarias y artísticas, tales como libros, *software*, música, obras fotográficas, obras plásticas y obras cinematográficas.
- *WIPO Performances and Phonograms Treaty* (Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas), que entró en vigor el 10 de mayo de 2002. Destinado a proteger los derechos de los productores de fonogramas, así como los derechos de los artistas, intérpretes o ejecutantes cuando sus obras se fijan en cualquier tipo de soporte.

Estas normas suponen un gran avance en la modernización de la legislación internacional, al dotar de mayor grado de protección a los derechos de los autores, y al establecer unos criterios y estándares básicos al desarrollo e implantación de las medidas de protección de la propiedad intelectual en los servicios de la Sociedad de la Información, llegando a ser comúnmente conocidos como los ñTratados sobre *Internet*ò

Ambos tratados exigen la creación de un marco de derechos básicos, que permita a los creadores ejercer un control y/o percibir una remuneración por las distintas formas en que se usan y disfrutan sus creaciones. Pero el factor más importante es la protección adecuada y eficaz que dichos tratados otorgan a los titulares de estos derechos, cuando sus obras se difunden empleando las nuevas tecnologías y sistemas de comunicación como *Internet*. En este sentido, los tratados establecen:

- Que el derecho de reproducción es de aplicación al entorno digital y al almacenamiento de material en formato digital en un medio electrónico.
- Que los titulares de los derechos pueden verificar si los distintos consumidores tienen acceso en línea a sus creaciones y en qué forma, por ejemplo, desde sus hogares a través de *Internet*.

Para mantener un equilibrio de intereses entre los titulares de los derechos y los consumidores, se específica que los países gozarán de flexibilidad para fijar excepciones o limitaciones a los derechos en el entorno digital, respecto de los usos considerados de interés público, para fines educativos y de investigación.

Esta normativa no regula de forma expresa los servicios de la Sociedad de la Información objeto de estudio en este informe -redes sociales y sitios *web* colaborativos-, ya que en el momento de aprobación de los mismos estos servicios avanzados aún no existían o se encontraban en una fase inicial.

En EE.UU. la norma básica en materia de protección de derechos de propiedad Intelectual es la *Digital Millenium Copyright Act* (en adelante, DMCA), de 28 de octubre de 1998, en la que se dispone la no responsabilidad de los prestadores de servicios de *Internet* o ISP respecto de la información transmitida, alojada o difundida por los usuarios a través de sus sistemas de información. Esta no responsabilidad, reconocida en la mayor parte de los Estados a nivel mundial, establece que será aplicable siempre que el prestador de servicios de *Internet*:

- No tenga conocimiento u obtenga beneficio económico de la actividad ilícita.
- Disponga de una política sobre propiedad intelectual publicada en su sitio *web*, que sea accesible por los usuarios.
- Cuente con un responsable que atienda las denuncias por infracción de derechos.

Normativa europea

A nivel europeo, dentro de las áreas legales de propiedad intelectual y nuevas tecnologías se encuentra la Directiva 2001/29/CE, del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información (Directiva 2001/29/CE), en virtud de la cual los Estados miembros establecen el derecho exclusivo a autorizar o prohibir la reproducción directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, por lo que se hace extensible a las Redes Sociales.

De igual forma, se dispone que los Estados miembros establecerán, en favor de los autores, el derecho exclusivo a autorizar o prohibir cualquier comunicación pública de sus obras.

Normativa nacional

Como la gran mayoría de normas de los países de nuestro entorno, la Ley de Propiedad Intelectual concede a los autores de las obras derechos en exclusiva sobre éstas, lo que supone que cualquier tratamiento, reproducción, puesta a disposición o transmisión de la obra deberá ser realizada con la autorización de los titulares de derechos. Tanto la normativa nacional, como la comunitaria, parten de un grado elevado de restricción de los derechos de explotación, de forma que nadie puede explotar derechos de propiedad intelectual sin autorización por parte del autor.

Desde el punto de vista normativo, España dispone de un gran elenco de normas encaminadas a la protección de los derechos de propiedad intelectual de los autores y, más específicamente, a la protección de la propiedad intelectual en los servicios de la Sociedad de la Información:

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (LPI), regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, modificado por la Ley 23/2006,de 7 de julio.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (LISI).
- Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Sin embargo, a pesar de que se trata de normas actualizadas recientemente, con el objeto de regular el uso que se realiza de los contenidos de propiedad intelectual a través de los servicios de la Sociedad de la Información, existen dificultades de aplicación a la hora de alcanzar la protección plena de los derechos de los autores, produciéndose situaciones en las que obras de propiedad intelectual son comunicadas públicamente o reproducidas sin contar con la autorización previa del autor.

Para minimizar estas situaciones, la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) dispone que ñlos prestadores de servicios de intermediación no tienen obligación de supervisar los contenidos que alojan, transmiten o clasifican en un directorio de enlaces, pero deben colaborar con las autoridades públicas, cuando se les requiera para interrumpir la prestación de un servicio de la sociedad de la información o para retirar un contenido de la Red. Pueden incurrir en responsabilidad si, conociendo la ilegalidad de un determinado material, no actúan con rapidez para retirarlo o impedir el acceso al mismoò

Las Redes Sociales como proveedores de servicios de *Internet* tienen la capacidad técnica de controlar los contenidos que en ellas se alojan. Por tanto, en principio cabe exigirles un deber general de control y supervisión de los contenidos ajenos, a modo de diligencia u observancia debido por el servicio que prestan.

Desde el punto de vista de la regulación penal para la protección de la propiedad intelectual, la Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, dispone tres conductas relacionadas con su protección:

- La distribución o comunicación pública de contenidos que están protegidos, ya sea mediante la distribución de copias físicas, o su puesta a disposición en *Internet* sin la autorización del titular de los derechos.
- La importación o fabricación de *software* o medios que permitan vulnerar las medidas de protección técnica incluidas en las obras, es decir, cualquier sistema que permita saltarse los sistemas anti-copia de un determinado soporte o página *web*.

En relación con la protección de la propiedad intelectual y las Redes Sociales, la relevancia penal que supone difundir públicamente contenidos de forma online y mediante tecnología P2P, así como la posibilidad de que se creen comunidades online encaminadas a la puesta a disposición de links para proceder a la descarga de obras de propiedad intelectual, ha sido analizada por parte de la Fiscalía General del Estado en su Circular 1/2006 ñSobre los Delitos contra la Propiedad Intelectual e Industrial tras la reforma de la Ley Orgánica 15/2003ò [52], donde se dispone que el intercambio de archivos a través de redes P2P no es constitutivo, en principio, de los requisitos necesarios para poder ser catalogado como un delito contra la propiedad intelectual, sin perjuicio de que pueda reunir los requisitos para ser considerado un ilícito civil.

El elemento clave para determinar la existencia de esta situación, es que en principio no exista un ánimo de lucro directamente relacionado con la actividad, requisito esencial dispuesto por la normativa vigente para poder ser considerado delito. No obstante, se establece que deberá atenderse a las circunstancias concretas de cada caso.

4.3.3. Posibles riesgos

Desde el punto de vista de los posibles riesgos que se pueden producir contra la protección de la propiedad intelectual en *Internet*, en general, y en los servicios de Redes Sociales, en particular, deben diferenciarse dos situaciones en origen:

- De un lado, cómo se ven afectados los contenidos que son titularidad de terceros y que el usuario decide publicar dentro de la Red Social sin autorización de los titulares del derecho de propiedad intelectual.
- De otro lado, las implicaciones jurídicas sobre las obras que sean titularidad de los propios usuarios y que éstos deciden compartir o hacer públicas a través de estas redes y plataformas.

El primer momento crítico para la protección de los derechos de propiedad intelectual respecto a los contenidos y obras elaboradas se encuentra en la fase inicial de registro del usuario, momento en el que éste acepta las condiciones de uso que en principio regirán toda su relación con la plataforma. El usuario debe leer, comprender y aceptar expresamente las condiciones de uso de la plataforma.

Aunque pudiera parecer que este hecho no reviste especial importancia resulta esencial, en la medida en que los usuarios aceptan con frecuencia condiciones de uso relativas a la protección en materia de propiedad intelectual, por las que ceden plenamente sus derechos de explotación a las plataformas para que los utilicen libremente durante el plazo máximo legal de 5 años.

Si a lo anterior se añade que la mayoría de las plataformas analizadas recogen condiciones de uso confusas, con redacciones frecuentemente extensas, de difícil comprensión y que habitualmente son alojadas en lugares del sitio *web* de difícil acceso para el usuario, se puede concluir que el número de usuarios que leen detenidamente y comprenden dichas condiciones legales no es alto.

Por consiguiente, es frecuente que la cesión de todos los derechos de propiedad intelectual de los contenidos creados a favor de la plataforma se realice de forma poco reflexiva, con lo que existe un posible riesgo para los usuarios que publican sus obras y creaciones en estas plataformas como medio de difusión.

El segundo momento en el que se pueden producir riesgos para los derechos de propiedad intelectual es en la fase de participación del usuario en la plataforma en la que puede publicar contenidos -propios o ajenos- para que sean compartidos con los demás usuarios de la Red Social. En este momento pueden plantearse varias situaciones:

- Que el contenido original haya sido creado por el propio usuario que lo publica. En estos casos, el usuario cede, en la mayor parte de los casos, sus derechos de explotación sobre la obra, sin apenas límite territorial, durante un plazo de 5 años -plazo legal máximo- y sin derecho a recibir ningún tipo de compensación por ello. Por lo tanto, se recomienda que el usuario valore a priori estas actuaciones que la Red Social puede realizar con dichos contenidos.

- Que los contenidos publicados sean propiedad de terceros. Cuando un usuario decide compartir dentro de la Red Social, ya sea con sus contactos o con toda la red, una determinada obra titularidad de terceros, no debe olvidar que la plataforma actúa en principio como mero intermediario, por lo que la responsabilidad de la publicación de dicho contenido recae directamente sobre el propio usuario.

Las Redes Sociales tienen una gran difusión y para los autores esta forma de distribuir contenidos puede ser muy ventajosa. Sin embargo, el principal problema que se puede plantear es que no hay formas efectivas de controlar y obtener una compensación directa por el trabajo realizado.

Por otro lado, y con independencia de la titularidad, existe el riesgo de que los contenidos (propios o ajenos) publicados por los usuarios en la plataforma puedan llegar a ser indexados por los motores de búsqueda de *Internet*, lo que conllevaría que la difusión fuese mayor y por tanto que el número de reproducciones aumentase de forma exponencial, incrementando, en consecuencia, de forma directa la compensación al titular de los derechos.

Por último, el tercer momento en el que los derechos de propiedad intelectual pueden verse sometidos a un posible riesgo derivado del uso realizado en las Redes Sociales, está en la fase de baja del servicio por parte del usuario. En principio todos los contenidos asociados al perfil del usuario: fotografías, vídeos, obras literarias, etc., serán eliminados o al menos se bloqueará el acceso a los mismos, en el momento en que el usuario solicite la baja del servicio o el bloqueo de su perfil.

4.3.4. Colectivos especialmente Vulnerables. Menores y discapacitados

Por lo que respecta al colectivo de menores e incapaces, el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (LPI) no establece ninguna especialidad respecto a los menores y el derecho de autoría, pudiendo ser autor de una obra de propiedad intelectual cualquier persona, con independencia de su edad.

Sin embargo, se ha de tener en cuenta que la normativa dispone que ñLos autores menores de dieciocho años y mayores de dieciséis, que vivan de forma independiente con consentimiento de sus padres o tutores o con autorización de la persona o institución que los tengan a su cargo, tienen plena capacidad para ceder derechos de explotación.ò

Será por tanto necesario que aquellas plataformas que aceptan el registro de menores de 18 años, soliciten a éstos que autentiquen su mayoría de edad o, en su caso, que viven de forma independiente conforme a los requisitos dispuestos en la legislación vigente.

4.3.5. Medidas empleadas para proteger los derechos de propiedad intelectual de los usuarios y de terceros

Como se ha mencionado en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) en España se emplea el sistema de denuncia de infracción de derechos de propiedad intelectual, mediante el cual el usuario puede notificar internamente a los administradores de la plataforma que existe una explotación no autorizada de derechos de propiedad intelectual, para que ésta pueda comprobarlo y en su caso retirar el contenido.

Existen acuerdos bilaterales con asociaciones de autores y grandes organizaciones propietarias de los derechos de explotación de las obras, mediante los cuales son los propios titulares de los derechos de explotación los que se encargan de vigilar, revisar y en su caso retirar los contenidos que vulneren sus derechos.

De igual forma, en los últimos tiempos se está observando como cada vez más las grandes compañías de la industria de contenidos están llegando a acuerdos bilaterales con las plataformas de difusión y Redes Sociales para abrir canales en los que alojar y publicar ellos mismos sus contenidos, como contramedida frente a la publicación indiscriminada y descontrolada de contenidos de su propiedad por parte de los usuarios. De esta forma no se evita que se publiquen en la red, pero sí se realiza el control de los contenidos publicados.

Este tipo de medidas suponen una representación clara de que el mercado está cambiando y de que los agentes intervinientes están comenzando a ver en la Sociedad de la Información una oportunidad y no un obstáculo, lo que sin duda alguna augura unos buenos resultados en los próximos años, tal y como expone el informe recientemente publicado por ASIMELEC, sobre ñLa Industria de los Contenidos Digitalesò[53].

Por su parte, el Tribunal de Justicia de las Comunidades Europeas ha afirmado que los Estados miembros al incorporar a sus sistemas legales las directivas que protegen los derechos de autor en la Sociedad de la Información deben garantizar un justo equilibrio entre los derechos a la protección de

datos personales, a la tutela judicial y a la propiedad (STJCE de 29/01/2008. Asunto C-276/06. *Promusicae* [54]).

Recientemente, el informe del Parlamento Europeo, que descartaba otorgar "poder policial" a los operadores de *Internet*, ha recibido el apoyo de la Comisión Europea, indicando que las operadoras "no pueden restringir el acceso de los internautas ni los derechos fundamentales de los ciudadanos sin una autorización judicial previaò[55], si bien la propuesta está pendiente de aprobación definitiva.

Del mismo modo, y desde el punto de vista público, en España, el Ministerio de Cultura, por acuerdo del Consejo de Ministros, aprobó el Plan integral del Gobierno para la disminución y eliminación de las actividades vulneradoras de la propiedad intelectual, publicado en el BOE de 26 de abril de 2005 [56], que se basa en la lucha contra la piratería.

La Industria Discográfica y Audiovisual ha formado lo que ellos mismos han venido a denominar ñLa Coalicióné formada por SGAE, *Promusicae* [54] (AIE y AGEDI), Federación para la Protección de la Propiedad Intelectual, la Asociación de Distribuidores Cinematográficos (ADICAN), la Asociación de Distribuidores de Vídeos (ADIVAN) y EGEDA, cuya finalidad está en fomentar la protección de los derechos de los autores que representan, mostrando especial atención a las vulneraciones que tienen su origen en los servicios de la Sociedad de la Información.

Por su parte, la Agencia Española de Protección de Datos ha formulado unas recomendaciones sobre la necesidad de aprobar una ley que permita proteger los derechos de autor de forma compatible con el derecho a la protección de datos personales [57].

4.4. Real Decreto Legislativo 1/2007. Ley de protección de los consumidores y usuarios

Los avances de las redes sociales y plataformas colaborativas están modificando las prácticas comerciales, redefiniendo la forma *online* de ofrecer bienes y servicios mediante la publicidad personalizada según los perfiles de usuario, diversificando el mercado y creando nuevos canales de distribución.

Estos nuevos modelos de negocio basados en el comercio electrónico pueden despertar un cierto grado de incertidumbre en los consumidores, en torno a cuestiones relativas a la seguridad de las

transacciones electrónicas, al perfeccionamiento y validez de los contratos, a la normativa aplicable o la jurisdicción competente en caso de litigio, entre otras cuestiones.

Los siguientes epígrafes profundizan en el análisis de estos aspectos informando acerca de los instrumentos normativos y medidas tecnológicas que existen actualmente al servicio de los usuarios/consumidores de bienes y servicios a través de *internet* para garantizar un entorno de tráfico económico seguro y confiable que garantice la total legalidad y transparencia en el proceso de compra de productos a través de i*nternet*, en general, o de cualquier Red Social o plataforma colaborativa, en particular, desde la que se opere.

4.4.1. Definición del derecho

Por consumidor se entiende ñtoda persona física o jurídica que interviene dentro de una actividad comercial, con el objeto de adquirir un producto o servicio a un precio determinado, bien sea a través de comercio habitual o mediante transacciones de comercio electrónicoò

A efectos de determinar qué se entiende por ñcontratos celebrados a distanciaò, hay que atender a la siguiente definición: ñlos contratos celebrados a distancia son aquellos celebrados con los consumidores y usuarios en el marco de una actividad empresarial, sin la presencia física simultánea de los contratantes, siempre que la oferta y aceptación se realicen de forma exclusiva a través de una técnica cualquiera de comunicación a distancia y dentro de un sistema de contratación a distancia organizado por el empresarioò[58].

La propia norma dispone una serie de medios a través de los que se pueden realizar prestaciones de servicios a distancia, siendo los más habituales: ñlos impresos, con o sin destinatario concreto, las cartas normalizadas, la publicidad en prensa con cupón de pedido, el catálogo, el teléfono -con o sin intervención humana- la radio, el teléfono con imagen, el videotexto con teclado o pantalla táctil, el correo electrónico, el fax y la televisiónò, entre otros.

Así, los derechos de los consumidores y usuarios, en lo que respecta a los contratos celebrados a distancia, tal y como dispone el Título III del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, comprenden los siguientes principios:

- Derecho de información.
- Derecho de desistimiento.
- Garantías mínimas del producto.
- Envío de comunicaciones comerciales y publicidad engañosa.

4.4.2. Marco jurídico aplicable

La normativa vigente aplicable al sector de consumidores y usuarios tiene por objeto salvaguardar los derechos de los usuarios y velar por el cumplimiento de las obligaciones impuestas entre las partes intervinientes.

Normativa internacional

A nivel internacional no se dispone de convenio expreso sobre la materia. Sin embargo, existen recomendaciones y guías de la OCDE procedentes de las distintas reuniones entre los ministros de comercio (y cargos asimilados) de los Estados. Entre ellas destaca la OECD *Consumer Protection Guidelines* (OCDE Guía de Protección de Consumidores), aprobada en septiembre de 1998 con una finalidad programática en la que se establecen los principios básicos para:

- Controlar las conductas comerciales fraudulentas.
- Solventar controversias y devolver objetos.
- Asegurar la privacidad de los datos del consumidor en las transacciones electrónicas.

En EE.UU., desde el punto de vista de los servicios de *Internet* en materia de protección de consumidores y usuarios, el órgano competente es la *Federal Communication Comission* (FCC) aunque, hasta la fecha, no se dispone de una regulación a nivel general para la defensa de este colectivo.

Normativa europea

A nivel europeo, la legislación vigente en materia de protección de consumidores y usuarios se encuentra dispuesta en cuatro Directivas:

- Directiva 93/13/CEE del Consejo, de 5 de abril, sobre las cláusulas abusivas en los contratos celebrados con consumidores.
- Directiva 99/44/CE, de 25 de mayo, del Parlamento Europeo y del Consejo, sobre determinados aspectos de la venta y las garantías de los bienes de consumo.
- Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo, relativa a la protección de los consumidores en materia de contratos a distancia.
- Directiva 85/577/CEE del Consejo, de 20 de diciembre, referente a la protección de los consumidores en el caso de contratos negociados fuera de los establecimientos comerciales.

Además hay que destacar la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior, objeto de transposición en España en la actual Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE), encargada de regular la prestación de servicios de la Sociedad de la Información.

Normativa nacional

Cronológicamente se debe referenciar la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, cuyo objeto de regulación son las ventas a distancia, estableciéndose que son aquel tipo de ventas que se realizan ñsin la presencia física simultáneaò de las partes, siempre que acciones esenciales del contrato, como la venta y la aceptación, se realicen por cualquier modo de comunicación a distancia y llevada a cabo dentro de un sistema de contratación organizado por el vendedor.

El Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, sin perjuicio de lo dispuesto por la LSSI-CE en lo que respecta a la contratación electrónica, dispone qué información debe figurar en las ventas a distancia de forma clara, comprensible e inequívoca, antes de iniciar el procedimiento de contratación:

- La identidad del vendedor o prestador de servicios y su dirección.
- Las características esenciales del producto o servicio.
- El precio, incluidos todos los impuestos.
- La forma de pago y modalidades de entrega o de ejecución.
- La existencia de un derecho de desistimiento o resolución y las causas del mismo.

- El coste de la utilización de la técnica de comunicación a distancia, cuando se calcule sobre una base distinta de la tarifa básica.
- El plazo de validez de la oferta y del precio.
- La duración mínima del contrato.
- En su caso, indicación de si el vendedor dispone o está adherido a algún procedimiento extrajudicial de solución de conflictos.

Cuando el usuario sea a la vez consumidor obtendrá inmediatamente los derechos contemplados en la legislación sobre consumidores y usuarios, que serán irrenunciables y ejercidos automáticamente, aunque la legislación aplicable no sea la española. Esto ocurrirá siempre y cuando el contrato presente un vínculo estrecho con cualquier Estado miembro, pudiéndose aplicar en este momento los principios recogidos en la LSSI-CE sobre el país de destino de la prestación de los servicios.

La contratación a distancia puede realizarse incluyendo condiciones generales de la contratación, las cuales tendrán que estar incorporadas al contrato, ser aceptadas por el usuario y firmadas o aceptadas por ambos contratantes. Las condiciones generales no primarán nunca sobre las específicas, salvo que las generales sean más beneficiosas para el adherente. Las dudas sobre las condiciones generales siempre se resolverán en sentido que favorezcan al adherente. En este sentido, se ha de partir de la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación (LCGC).

El uso de condiciones generales de contratación es frecuente en los procedimientos de contratación online. Se trata de contratos de adhesión en los que los usuarios/consumidores no disponen de ningún tipo de capacidad de decisión y variación del clausulado, debiendo aceptar, en todo caso, las condiciones que el empresario hubiera dispuesto. Es por esto que la normativa vigente pretende aumentar el grado de protección de los usuarios/consumidores de este tipo de procedimientos de suscripción a servicios.

No se incorporarán al contrato las cláusulas generales que el adherente no haya tenido oportunidad real de conocer plenamente en el momento de celebrar el contrato o que no hayan sido firmadas en virtud del artículo 7 de la LCGC. Por eso, en los contratos electrónicos, es importante remarcar su existencia y ubicación, tanto en el momento de la firma del mismo, como antes de la iniciación del proceso de firma. Además, las cláusulas deberán ser legibles, claras, simples y comprensibles, para no correr el riesgo de nulidad recogido en el artículo 8 de la LCGC. Cuando una serie de cláusulas sean consideradas nulas, pero con las restantes y las particulares el contrato pueda seguir subsistiendo, éste no será considerado ineficaz.

Por último cabe resaltar lo dispuesto por la normativa específica para la regulación del comercio electrónico en España, concretamente en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE), en la que se dispone que ñlos contratos celebrados por vía electrónica producirán todos los efectos cuando concurran el consentimiento y los demás requisitos necesarios para su validezò Además, se regirán por el Código Civil, el Código de Comercio y las leyes referenciadas anteriormente.

4.4.3. Posibles riesgos

En algunos casos los posibles riesgos a los que se puede enfrentar un consumidor -como usuario de redes sociales- pueden ser asumidos por el propio usuario, ya que es él mismo quien mantiene el control de la información alojada en la plataforma o Red Social en la que, de forma voluntaria, se ha registrado.

En función de su actividad, todo proveedor establecido en España debe cumplir con ciertas obligaciones que la LSSI-CE establece con el fin de garantizar que su actividad se realice con total transparencia, sin vulnerar los derechos de los usuarios.

Así, el artículo 10 LSSI-CE recoge una serie de obligaciones a cargo de los prestadores de servicios de la Sociedad de la Información, con el objeto de preservar el derecho de información a consumidores y usuarios respecto de los bienes o servicios que les son proporcionados. En concreto, se debe informar del:

- Nombre o denominación social, domicilio, dirección de correo electrónico y cualquier otro dato que permita establecer una comunicación directa y efectiva.
- Los datos de inscripción en el Registro Mercantil.
- Datos relativos a autorizaciones, en caso de estar sujeto a ello.
- Si ejerce una profesión regulada deberá indicar: datos del colegio profesional, titulación académica oficial, lugar de expedición y homologación, y si fuere el caso, normas profesionales aplicables al ejercicio de su profesión.
- El número de identificación fiscal que le corresponda.
- Información clara y exacta sobre el precio del producto o servicio, indicando si incluyen o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

- Los códigos de conducta a los que esté adherido.

Otro posible riesgo con el que se puede encontrar un consumidor en el momento de manifestar su interés por contratar un determinado servicio ofrecido a través de una Red Social es el referido a la publicidad engañosa, que consiste en aquella manifestación de publicidad ilícita llevada a cabo en cualquier forma que induce o puede inducir a error a sus destinatarios, pudiendo afectar a su comportamiento económico.

En este sentido, la Ley 34/1988, de 11 de noviembre, General de Publicidad determina todos los elementos que caracterizan la publicidad engañosa (características de los bienes, precio, condiciones de contratación y motivo de la oferta).

La aceptación de las condiciones generales de contratación constituye otro aspecto fundamental a tener en cuenta por el consumidor antes de formalizar la contratación del servicio ofrecido a través de una Red Social. Como se ha señalado, la propia legislación establece la obligación de informar al usuario de forma clara y precisa sobre las condiciones a las que están sometidas las partes dentro de la relación contractual.

No obstante, la aparición de cláusulas abusivas en un contrato constituye un defecto con implicaciones jurídicas trascendentales entre las partes. La propia normativa define como cláusula abusiva la siguiente: ñTodas aquellas estipulaciones no negociadas individualmente y todas aquellas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe, causen en perjuicio del consumidor y usuario un desequilibrio importante de los derechos y obligaciones de las partes que se deriven del contratoò

En cualquier caso, toda cláusula contractual que limite los derechos básicos de los consumidores y usuarios que sea notoriamente desproporcionada en relación con el prestador o que prive del goce de los derechos que la propia normativa le concede, tendrá el carácter de cláusula abusiva.

El desarrollo de las nuevas tecnologías, unido al crecimiento de la actividad comercial a través de *Internet*, ha dado lugar a nuevas prácticas abusivas derivadas del incumplimiento en las disposiciones legales que, en casos más extremos, derivan en la comisión de delitos sancionados por la normativa penal.

4.4.4. Colectivos especialmente Vulnerables. Menores y discapacitados

La LSSI-CE establece que, en el caso de páginas *web* accesibles por menores, éstas no deben integrar contenidos que atenten contra los mismos, y que además la protección de la infancia y de la juventud tiene que ser uno de los valores que rija el entendimiento de toda la norma.

Actualmente existen mecanismos -programas informáticos de filtrado y bloqueo- de especial utilidad para controlar y restringir los contenidos o materiales a los que pueden acceder los menores.

En todo caso, es conveniente acompañar a los menores en su navegación por la Red, sobre todo, en los casos en los que se disponga de suscripciones a servicios *premium* o de pago.

4.4.5. Medidas empleadas para proteger los derechos de los consumidores y usuarios

Actualmente las medidas empleadas por las Redes Sociales que operan como sitios de comercio electrónico o que pueden verse sometidos a la normativa de consumidores son los **sistemas de identificación electrónica** basados en certificados de firma electrónica reconocida que están comenzando a ser utilizados por las plataformas de comercio electrónico como medio para garantizar las transacciones comerciales que los consumidores realizan. La implementación y uso de este tipo de sistemas permiten tanto al consumidor como a la tienda de comercio electrónico garantizar:

- La identidad de la persona que compra y la que vende.
  - La integridad del consentimiento prestado.
  - El ñno repudioòde la transacción.

De esta forma, cualquier usuario/consumidor que compre a través del sitio *web*:

- Tiene plena seguridad de que el titular del nombre de dominio y de la tienda online es la compañía que realmente vende los productos o presta los servicios.
- Puede demostrar que un día concreto, a una hora específica prestó su consentimiento y abonó una cantidad determinada a cambio del envío de un producto.
- Por otro lado, el vendedor cuenta con:

- La capacidad tecnológica de acreditar la fecha y hora del consentimiento prestado electrónicamente por parte del usuario.
- La aceptación por parte del usuario/consumidor de las condiciones generales de contratación expuestas en el sitio *web*.
- En el caso de que el usuario niegue que fue él quien prestó el consentimiento requerido será carga suya el demostrarlo, reflejándose así el ñno repudioòanteriormente mencionado.

Es esencial tener en cuenta que la implantación plena de este tipo de sistemas de identificación electrónica se encontrará totalmente aplicada en el momento en el que el DNI electrónico (DNIe) esté más expandido ya que ofrece la imposibilidad de su falsificación evitando la suplantación de la identidad, problemática mencionada anteriormente.

Del mismo modo, la gran mayoría de las plataformas analizadas que cuentan con procedimientos de compra electrónica recurren a la instalación en sus servidores de un protocolo de puerto seguro, (*Secure Socket Layer* o *SSL*), que garantiza a todos sus usuarios que las comunicaciones, solicitudes e informaciones transmitidas entre el sitio *web* y el usuario no son accesibles por parte de terceros no autorizados.

De igual forma, todas las plataformas que integran comercio electrónico disponen de una Terminal Punto de Venta ï TPV- de pago electrónico proporcionada por una entidad financiera, que somete todo el procedimiento de pago electrónico a un protocolo de seguridad debidamente certificado y que garantiza que el establecimiento no tiene acceso, ni conserva, ni trata los datos de tarjeta de los usuarios.

Por otro lado, se ha detectado la evolución clara por parte de las plataformas en relación al empleo de medios de pago alternativos que garanticen plenamente la seguridad de las transacciones y que prevean seguros de responsabilidad para el caso de que el producto no se reciba o la transacción sufra algún tipo de error.

Supone una garantía para el usuario/consumidor de bienes y servicios de una Red Social, la puesta a su disposición de las condiciones generales de contratación, donde se disponen todas las cláusulas relativas a las garantías, plazos de devolución, precios, transportes, entre otras. No obstante, actualmente esta garantía no se encuentra totalmente implementada, al no disponer de documentos legales que cumplan de forma estricta con las obligaciones dispuestas en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

4.5. El derecho al olvido

Las nuevas tecnologías de la información y las comunicaciones, han propiciado que miles de millones de datos personales puedan ser almacenados indefinidamente en la *web*. La eficacia de los buscadores, permiten localizar estos datos y hacerlos accesibles a cualquier ciudadano, mediante una búsqueda, como reacción a esta situación ha nacido lo que se conoce como derecho al olvido. El problema radica en que es muy fácil perder el control de la información que se publica en la *web.*

4.5.1. Definición del derecho

Se puede definir como las iniciativas y medios llevados a cabo para suprimir o bloquear la publicación de datos personales en *internet*, al considerar que afectan a la privacidad y/o dignidad humana, exigiendo que no se publiquen en ningún sitio de la red.

No obstante no siempre es factible aplicar tecnologías que impidan la indexación de datos, en muchos casos la información personal provienen de una fuente pública, como Boletines Oficiales, y no es razonable el borrador de dicha información, ni el bloqueo de toda la información publicadas en los mismos, aunque si se puede actuar parcialmente.

El procedimiento que se suele seguir es reclamar ante el buscador, acudir a la Agencia de Protección de Datos cuando no se obtiene contestación o esta es denegatoria, para terminar en los tribunales [59].

Un ejemplo sería el de un joven de 20 años que cuelga en *Tuenti* un video bañándose desnudo en una playa de madrugada. Puede resultar divertido en su momento y para su entorno, de modo que este joven elimina el contenido de *Tuenti* cuando lo considera oportuno. No obstante, el video podría haber pasado ya a otra red, como *Youtube*, y ser lo bastante público como para encontrarlo en *Google* a través de su nombre. En el futuro, en un ámbito distinto (como el laboral), la difusión de este video podría tener un impacto muy negativo en la vida diaria de esta persona [60].

4.5.2. Marco jurídico aplicable

El reconocimiento de este 'derecho al olvido' se incluirá en la reforma de las normas de protección de datos de la UE, que tiene como fin adaptarlas a los cambios provocados por las nuevas tecnologías.

Al modificar la presente legislación, se intenta clarificar específicamente que las personas deben tener el derecho, y no sólo la posibilidad, de retirar su consentimiento al procesamiento de datos. Por ello, el primer pilar de la reforma será el 'derecho a ser olvidado': un conjunto completo de reglas nuevas y existentes para afrontar mejor los riesgos para la privacidad en Internet".

También se propone la exigencia de que la configuración de redes las sociales garantice la "privacidad por defecto", de forma que los datos de los usuarios no puedan procesarse salvo si éstos han dado su permiso expreso.

La regla de la óprivacidad por defectoô evitaría la recogida de datos a través de aplicaciones de *software*, por ejemplo.

Por ello, Bruselas exigirá una mayor transparencia a las Redes Sociales, que estarán obligadas a informar a los usuarios sobre los datos que recogen, con qué objetivos lo hacen, cómo pueden ser usados por terceras partes y cuáles son los riesgos para que los usuarios no pierdan el control sobre su información personal.

Finalmente, la Comisión obligará a que las empresas situadas fuera de la UE que procesen datos de ciudadanos comunitarios cumplan también estas reglas [61].

CAPÍTULO 5

CONCLUSIONES Y LINEAS FUTURAS

5. CONCLUSIONES Y LÍNEAS FUTURAS

No cabe duda que las Redes Sociales están suponiendo un gran avance que permiten la relación entre las personas independientemente de la zona geográfica, gracias a todas las herramientas integradas en las mismas. El fenómeno de las Redes social es gracias al surgimiento de la *Web 2.0*, a través de la cual los internautas pueden generar contenido *web*, subir archivos y personalizar su navegación. También el método de crecimiento empleado por este tipo de plataformas basado principalmente en el ñ*boca a boca***ò** *(o* crecimiento viral*),* ha permitido en poco tiempo la expansión de estos servicios. Se puede por ello tener una vida social totalmente activa. Las conductas sociales de relaciones humanas están experimentando por tanto un gran cambio, especialmente entre los más jóvenes. Ahora mucha gente pasa horas enteras viendo fotos y videos de sus amigos, o buscando trabajo sin salir de casa. En el ámbito empresarial se utiliza para favorecer y fomentar las relaciones entre los empleados generando mayores beneficios para las empresas y fundamentalmente para el *marketing*. En definitiva un buen uso de las Redes Sociales generan mayores ventajas y beneficios que aquellas organizaciones que se basan en el modelo tradicional de negocio. En la enseñanza estos nuevos canales de comunicación se están poniendo también muy de moda y es conocida como enseñanza *B-learning* (semi-presencial), fomentando la comunicación entre profesores y alumnos, aumentando la autonomía de los estudiantes y ayudando al profesor a gestionar sus contenidos de forma centralizada.

Pero desafortunadamente el crecimiento y notoriedad de estos espacios sociales no queda exento de posibles riesgos o ataques malintencionados. Esto es debido, en parte, a que el uso de estas redes se basa en la publicación de información personal de los usuarios, hecho que puede generar situaciones que amenacen y vulneren derechos fundamentales no sólo del propio usuario, sino incluso de terceros.

Así, por ejemplo, la libre difusión de información de un usuario puede vulnerar, entre otros, los derechos de protección del honor, la intimidad, la propia imagen y los datos de carácter personal. Hay que tener en cuenta, no obstante, que en muchas ocasiones esta difusión se debe a una falta de formación y conocimiento del usuario, que realiza una mala configuración de la privacidad en su perfil.

El riesgo de vulneración aumenta cuando la información que se publica no es la de uno mismo sino la de terceros y alcanza su máximo cuando el usuario de la Red Social es un menor, ya que a los anteriores riesgos hay que añadir el del acceso a contenidos inapropiados y el del posible contacto con adultos malintencionados.

No obstante, debe tenerse en cuenta la existencia en España de regulación específica encargada de tratar los aspectos relacionados con los prestadores de servicios de la Sociedad de la Información [62]. Por un lado, la aplicación de la Directiva 95/46/CE, teniendo en cuenta que estas actividades entran en el ámbito de aplicación de la normativa, y por otro, la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico dispone en su artículo 5, los aspectos concretos que aplican a los *ñPrestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo,ò* al señalar que aquellos *ñé que dirijan sus servicios específicamente al territorio español quedarán sujetos, ade*más, *a las obligaciones previstas en esta Ley, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicablesò*

En cualquier caso, es importante señalar que las compañías propietarias de Redes Sociales deben mejorar:

Desde el punto de vista jurídico:

Las redes analizadas disponen de información legal en la que existen algunas carencias entre las que destacan:

- Las condiciones de uso son alojadas habitualmente en lugares del sitio *web* de difícil acceso para el usuario.
- Son confusas y con redacciones frecuentemente extensas.
- Resultan de difícil comprensión para cualquier usuario medio que no disponga de conocimientos jurídicos y tecnológicos.
- Insuficiente respecto a los medios de seguridad tecnológicos existentes en la plataforma.

Desde el punto de vista tecnológico:

Las Redes Sociales deben avanzar en el uso de las siguientes medidas técnicas:

- Formación a los usuarios sobre los diferentes aspectos de configuración del perfil y las ventajas de una adecuada restricción en la difusión de datos personales.
- Cambios en la configuración por defecto del nivel de privacidad (generalmente está configurado permitiendo la máxima difusión de los perfiles).
- Control de la indexación y almacenamiento de los perfiles por parte de los buscadores.

- Las redes no han implementado sistemas para identificar la edad de los usuarios, a pesar de que en la actualidad existen diferentes proyectos116 con este objetivo.
- Establecer sistemas de identificación remota de usuarios mediante sistemas de firma electrónica reconocida. Sistemas como el DNIe permitirían asegurar las transacciones electrónicas y supondría que todas las comunicaciones realizadas de forma *online* contasen con la garantía de integridad plena, detectándose cualquier tipo de variación que hubiera podido sufrir durante su envío.

Así por tanto destacar la gran importancia de las instituciones gubernamentales que tienen la obligación de publicar nuevas leyes mejor adaptadas a este fenómeno social.

Como futuras líneas de investigación podemos citar:

- Estudio sobre la creación de mecanismos más fiables y robustos de verificación y validación de la edad de los usuarios que acceden a las Redes Sociales.
- Estudio de los comportamientos psicológicos ante un importante acontecimiento social, deportivo, político, etc. en las plataformas sociales.
- Estudio sobre la importancia de incluir una asignatura relacionada con los riesgos en *internet* en el plan de estudios nacional.
- Estudio sobre pautas y guías a seguir por parte de las empresas para aprovecharse lo máximo posible el poder *Social Media.*

Resaltar por último la desviación temporal en el desarrollo del proyecto y que explicamos en el siguiente apartado.

CAPÍTULO 6

PRESUPUESTO

6. PRESUPUESTO

6.1. Introducción

En este apartado se muestran las fases y sub-fases del proyecto junto con el correspondiente diagrama de Gantt y un desglose de costes de personal, costes del material y costes totales.

6.2. Planificación final

El siguiente diagrama *Gantt* (ver figura 9) muestra el desarrollo desde el inicio al fin de todo el PFC. Cabe destacar los 2 principales hitos para la consecución del mismo dentro de la tarea ôESTUDIO Y DOCUMENTACIÓNô

- Recopilación y estudio del estado del arte. El 8 de noviembre de 2011 (total 105 días) finaliza el estudio de toda la información relativa a las redes sociales en cuanto a definición, seguridad y legislación.
- Unificación y clasificación de la información obtenida para el desarrollo de los diferentes apartados del PFC (total 20 días). Se unifica y se extrae la información más relevante para el PFC.

La duración total del PFC ha sido de 294 días, o lo que es lo mismo de 9,8 meses (domingos festivos). El trabajo dedicado al PFC por cada jornada diaria ha sido de 2 horas, lo que hace un total de 588 horas.

Destacar que la finalización prevista para el proyecto era para el pasado día 15 de Mayo de 2012 (ver figura 8), pero debido a la basta documentación e investigación realizada y la dificultad para plasmar y cumplir con los objetivos iniciales del proyecto, se vio en la imperiosa necesidad de ampliar la tareas ô*Unificación y selección de la documentación*ôy ô*Desarrollo de los apartados del PFC*ôen 4 y 20 días mas respectivamente a lo que estaba previsto en un principio.

Figura 8. Planificación inicial PFC (Ver zoom 300%).

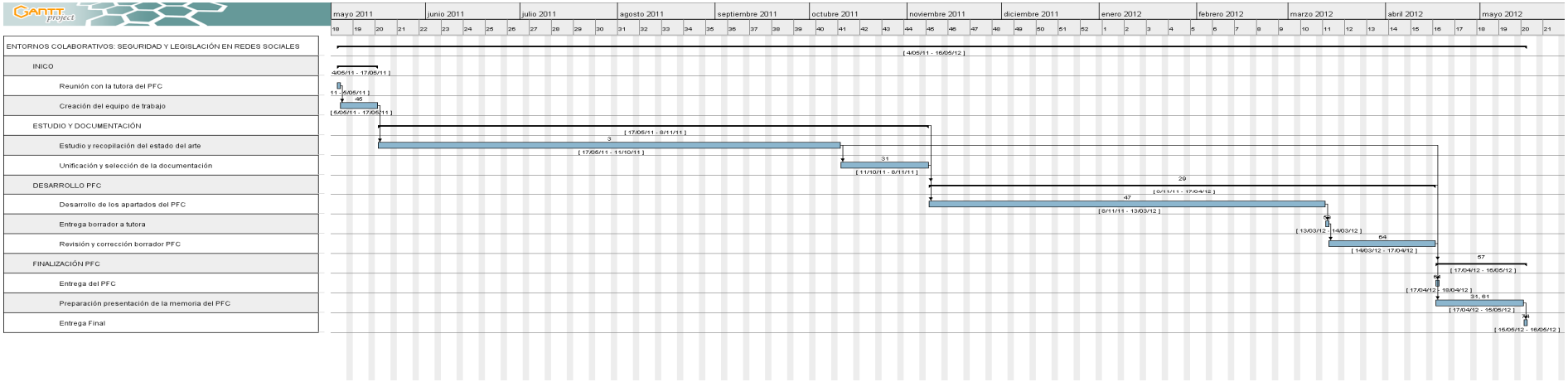
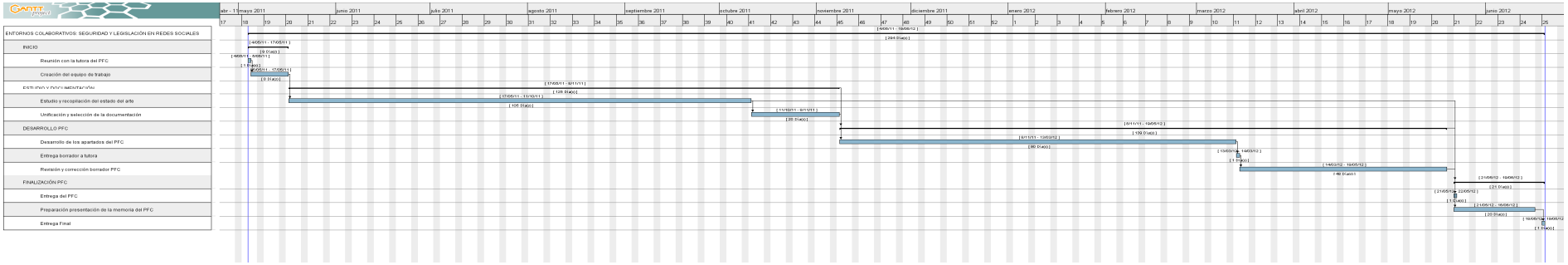


Figura 9. Planificación final PFC (Ver zoom 300%).



6.3. Presupuesto

Para detallar el presupuesto del PFC se ha utilizado la plantilla protocolaría utilizada para los Proyectos Fin de Carrera en la Escuela Politécnica de la Universidad Carlos III de Madrid.

Figura 10. Presupuesto PFC (Ver zoom 230%).

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor: Víctor Manuel Pérez García

2.- Departamento: Informática.

3.- Descripción del Proyecto: Proyecto de Fin de Carrera
- Título: ENTORNO COLABORATIVOS: SEGURIDAD EN REDES SOCIALES
- Duración (meses): **9,8**
Tasa de costes Indirectos: **21%**

4.- Presupuesto total del Proyecto (valores en Euros):
Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	Titulación - solo a título informativo	Categoría	Dedicación	(hombres mes) [a]	Coste hombre mes	Coste (Euro)	Firma de conformidad
Pérez García, Víctor Manuel		Ingeniero Técnico		9,8	600,00	5.880,00	
						0,00	
						0,00	
			Hombres mes	**9,8**	**Total**	5.880,00	

[a] **1 Hombre mes = 60 horas.** Máximo Anual de dedicación de 12 hombres mes 720
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (528 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d]
Equipo informático	500,00	100	9,8	60	81,67
Pantalla panorámica 17''	200,00	100	**9,8**	60	32,67
					0,00
					0,00
					0,00
				Total	114,33

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} \times C \times D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación (60 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
	Total	0,00

OTROS COSTES DIRECTOS DEL PROYECTO[e]

Descripción	Empresa	Costes imputable
	Total	0,00

[e] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas, otros,...

6.- Resumen de costes

Presupuesto Costes Totales	**Presupuesto Costes Totales**
Personal	5.880
Amortización	114
Subcontratación de tareas	0
Costes de funcionamiento	0
Costes Indirectos	1.156
Total	7.150

El presupuesto total de este proyecto asciende a la cantidad de **7.150 euros.**

CAPÍTULO 7

GLOSARIO

7. GLOSARIO

ADICAN: Asociación de Distribuidores Cinematográficos.

ADIVAN: Asociación de Distribuidores de Vídeos.

AEPD: Agencia Española de Protección de Datos.

AGEDI: Asociación de Gestión de Derechos Intelectuales.

AIE: Entidad de Gestión de los derechos de Propiedad Intelectual.

APEC: Cooperación Económica del Asia-Pacífico.

ARCO: Acceso, Rectificación, Cancelación y Oposición, derecho que tiene cada ciudadanos en referencia a sus datos personales.

ARP *(Address Resolution Protocol):* Protocolo de Resolución de Direcciones.

ARPA *(Advanced Research Projects Agency):* Agencia de Investigación de Proyectos Avanzados de los Estados Unidos.

ARPANET *(Advanced Research Projects Agency Network):* Red de ordenadores creada por la ARPA para permitir la comunicación entre los diferentes organismos del país.

ASIMELEC: Asociación de Empresas del Sector TIC, las Comunicaciones y los Contenidos Digitales.

ATP (*Advanced Persistent Threat*): Amenazas avanzadas persistentes.

BITNET *(Because It's There NETwork):* Porque está ahí la red.

CAPTCHAS *(Completely Automated Public Turing test to tell Computers and Humans Apart)*: Prueba de *Turing* (Prueba de Inteligencia) pública y automática para diferenciar máquinas y humanos.

CDA *(Communications Decency Act):* Ley de Decencia en las Telecomunicaciones.

CE: Comunidad Europea.

CE: Constitución Española.

CEDH: Comisión Europea de Derechos Humanos.

CEE: Comunidad Económica Europea.

CERT *(Computer Emergency Response Team):* Equipo de Respuesta de Emergencias Informáticas, igual que la CSNET.
CIDR *(Classless Inter-Domain Routing):* Enrutamiento entre dominios sin Clases

CMC: Comunicación mediante computadora.

CSNET *(Computer Emergency Response Team):* Equipo de Respuesta de Emergencias Informáticas.
DARPA *(Defense Advanced Research Projects Agency):* En 1972 ARPA pasa a llamarse DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa).
DMCA *(Digital Millenium Copyright Act):* Protección de Derechos de Propiedad Intelectual.

DNS *(Domain Name System): S*istema de Nombres de Dominio.

DoS *(Denial of Service):* Denegación de Servicio.

EEUU (*United States of America*): Estados Unidos de América.

EFF *(The Electronic Frontier Foundation): Fundación de la Frontera Eléctrica de los EEUU.*

EGEDA: Entidad de Gestión de Derechos de los Productores Audiovisuales.

EGP *(Exterior Gateway Protocol):* Protocolo de enrutamiento de *gateway* (puerta de enlace) exterior.
ENISA *(The European Network and Information Security Agency):* Red Europea de Información y Seguridad.
EUNET *(The European Network):* Red de Usuarios Europeos.

EV-SSL *(Extended Validation-Secure Socket Layer):* Certificado de Validación Extendida.

FCC (*Federal Communication Comission*): Comisión Federal de Comunicación.

HTLM *(HyperText Markup Language):* Lenguaje de Marcado de Hipertexto.

HTTP *(Hypertext Transfer Protocol):* Protocolo de Transferencia de Hipertexto.

IAD *(Internet Addiction Disorder):* Adicción a *Internet*.

IBM *(International Business Machines):* Compañía Internacional de Ordenares

IGP *(Interior Gateway Protocol):* Protocolo de enrutamiento de *gateway* (puerta de enlace) interior.

INTECO *(National Communications Technology Institute):* Instituto Nacional de las Tecnologías de la Comunicación.

INTERNIC *(Internet* Network Information Center*): Centro de Información de Red de Internet.*

IP *(Internet Protocol):* Protocolo de *internet* para la comunicación de datos a través de una red.

ISP *(Internet Service Provider):* Proveedor de servicios de Internet

ISTTF *(Internet Safety Technical Task Force):* Grupo de Trabajo Técnico en la Seguridad de Internet.

LAN *(Local Area Network):* Red de Área Local.

LAND *(Local Area Network Denial):* Red de Area Local. Es un ataque de red que se efectúa a través de una usurpación de dirección IP.

LCGC: Ley de Condiciones Generales de la Contratación.

LISI: Ley para el Impulso de la Sociedad de la Información

LOPD: Ley Orgánica de Protección de Datos.

LPI: Ley de Propiedad Intelectual.

LSSI-CE: Servicios de la Sociedad de la Información y del Comercio Electrónico

MILNET *(Military Network):* Red Militar.

MIT *(Massachusetts Institute of Technology):* Instituto Tecnológico de Massachusetts.

MitM *(Man In The Middle):* Intermediario*.*

NASA *(Nacional Aeronautics and Space Administration):* Agencia Espacial de los EEUU.

NCP *(Network Control Protocol):* Protocolo de Control de Red.

NCSA *(Supercomputing Aplications):* Aplicaciones Computarizadas.

NSF *(National Science Foundation):* Fundación Nacional de la Ciencia de los EEUU.

NSFNET (*National Science Foundation's Network):* Fundación Nacional de la Ciencia y las redes de los EEUU.

NWG (*Network Working Group):* Grupo de trabajo de redes liderado por liderado por *S.Crocker* que acabó el protocolo *host* a *host* inicial para ARPANET

OCDE: Guía de Protección de Consumidores.

OCDE: Organización para la Cooperación y Desarrollo Económico.

OECD *(Consumer Protection Guidelines)*: OCDE en inglés.

OMPI: Organización Mundial de la Propiedad Intelectual.

ONU: Organización de las Naciones Unidas.

OTP *(One Time Password):* Contraseñas de un sólo uso.

OWA: *Outlook web Access.*

P2P *(peer to peer):* Comunicación entre iguales que significa que los ordenadores que se comunican mediante P2P se comunican directamente entre si sin la intervención de un servidor central.

P3P *(Platform for Privacy Preferences)**:*** Plataforma de Preferencias de Privacidad.

PET: Protección del Derecho a la Intimidad.

PKI *(Public Key Infrastructure):* Infraestructura de Clave pública.

POD *(Ping On Death):* Ping de la muerte.

PRIME *(Privacy and Identity Management for Europe):* Privacidad y Gestión de Identidad para Europa.

RDLOPD: Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

REPLAY: Es una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada.

Smurf: Es un ataque de denegación de servicio que utiliza mensajes de ping al *broadcast* con *spoofing* para inundar un objetivo (sistema atacado).

SQL *(structured query language):* Lenguaje de consulta estructurado.

SSL *(Secure Socket Layer):* Protocolo de Capa de Conexión Segura. El protocolo SSL es un sistema diseñado y propuesto por *Netscape Communications Corporation*.

STC: Comité de Protección Civil.

SYN: Es un *bit* de control dentro del segmento *TCP*, que se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión en el procedimiento de establecimiento de tres fases (*3 way handshake*).
TCP/IP *(Transmission Control Protocol/Internet Protocol):* Protocolo de control de transmisión/Protocolo.
TPV: Terminal Punto de Venta.

UCLA *(University of California, Los Angeles):* Universidad de California en la que estudió *Michel Eli*e, uno de los pioneros de la creación de *internet.*
UE: Unión Europea.

URL *(Uniform Resource Locator):* Localizador de Recursos Uniformes.

US-CERT *(Current Activity - Malicious Code Targeting Social Networking Site Users).*

USENET *(Users Network): Red de Usuarios.*

VPN/RAS2: Es un sistema para simular una red privada sobre una red pública, por ejemplo, *Internet*. La idea es que la red pública sea "vistaò desde dentro de la red privada como un cable lógico que una las dos o más redes que pertenecen a la red privada).
WEB *(World Wide web):* Red Global Mundial.

WIPO *(World Intellectual Property Organization):* Organización Mundial de la Propiedad Intelectual.
WIPO: Organización Mundial de la Propiedad Intelectual.

XSS *(Cross-site scripting):* Es un tipo de inseguridad informática o agujero de seguridad basado en la explotación de vulnerabilidades del sistema de validación de HTML incrustado.
YAHOO! : Motor de búsqueda en *Internet.*

CAPÍTULO 8

REFERENCIAS

8. REFERENCIAS

Referencias documentación:

[00].Definición de Red Social en la *Wikipedia*, la enciclopedia de Internet: http://es.wikipedia.org/wiki/Red_social

[01].Número total de usuarios de redes sociales en todo el mundo:

https://www.unience.com/es/users/emiliomarquez/blog/2010/03/25/940-millones-de-usuarios-de-redes-sociales-en-todo-el-mundo

[02].Número total de usuarios Redes Sociales en España. Disponible *[Internet]*:

http://www.concepto05.com/2012/01/estadisitica-usuarios-de-redes-sociales-en-espana-2012/

[03].33 Conferencia Internacional de Autoridades de Protección de datos y privacidad. Disponible *[Internet]*:

http://www.apep.es/apep-y-la-33-conferencia-internacional-de-autoridades-de-proteccin-de-datos-y-privacidad/

[04].Teoría de los de los 10 saltos. Disponible *[Internet]*:

http://www.editum.org/Que-Son-Las-Redes-Sociales-En-Internet-p-316.html

[05].Otras definiciones de Redes Sociales. Disponible *[Internet]*:

http://www.slideshare.net/CONDOR_NET/confidencialidad-de-datos-en-redes-sociales

[06].Origen de Internet: http://www.maestrosdel*web*.com/editorial/internethis/

[07].Primeras Redes Sociales:

http://www.slideshare.net/norbecchio/breve-historia-de-las-redes-sociales-9650295

[08].Comunicación Síncrona y Asíncrona. Disponible *[Internet]*:

http://www.fernandoplaza.com/2009/03/comunicacion-sincrona-vs-comunicacion-asincrona-2.asp

[09].La importancia de las Redes Sociales. Disponible *[Internet]*:

http://mcdilo.blogspot.com/2009/03/la-importancia-de-las-redes-sociales-en.html

[10].Ventajas para las Empresas. Disponible *[Internet]*:

http://www.coguanpostshare.es/ventajas-de-las-redes-sociales-para-tu-empresa/

[11].Chantaje en Facebook, disponible *[Internet]*: http://uimpi.net/entry/noticia/77771/chantajista-de-facebook-condenado-a-15-anos.html

[12].Adicción a las Redes Sociales, disponible *[Internet]*:

http://www.psicologia-online.com/colaboradores/nacho/ainternet.htm

[13].Tipología de Redes Sociales, disponible *[Internet]*:
http://www.slideshare.net/crepusculo/clasificacion-de-las-redes-sociales

[14].Disponible *[Internet]*:

- http://www.professionalpartners.es/servicios/social_smo
- http://www.reaprendermarketing.com/2011/06/la-empresa-que-no-dialogue-con-los.html

[15].Disponible *[Internet]*:
https://www.agpd.es/portal*web*AGPD/canaldocumentacion/conferencias/common/pdfs/30_conferencia_internacional/resolucion_redes_sociales.pdf

[16].Disponible *[Internet]*:

http://www.estefaniasantos.com.ar/index.php?view=article&id=68%3Ala-seguridad-en-las-redes-sociales&option=com_content&Itemid=53

[17].Disponible *[Internet]*:

http://www.eweekeurope.es/noticias/noticias-seguridad/la-seguridad-de-las-redes-sociales-en-entredicho-543

[18].Artículo amenazas de seguridad en Redes Sociales. Disponible *[Internet]*:

- http://www.eweekeurope.es/noticias/la-seguridad-de-las-redes-sociales--en-entredicho-581
- http://technology.timesonline.co.uk/tol/news/tech_and_*web*/the_*web*/article5834638.ec
- http://www.elpais.com/articulo/internet/Facebook/Hi5/sufren/ataque/masivo/phising/elpeputec/20080625elpepunet_7/Tes
- http://www.internetyderecho.com/etiqueta/suplantacion-de-identidad/
- http://www.hoytecnologia.com/noticias/Registrada-primera-denuncia-suplantacion/97003
- http://www.us-cert.gov/current/index.html#malicious_code_targeting_social_networking
- http://www.us-cert.gov/cas/tips/ST06-003.html
- http://therooter.com/2008/08/tips-consejos-de-seguridad.html
- http://es.kioskea.net/contents/attaques/attaques.php3

[19].El *OpenID* y el desarrollo de un nuevo sistema blando de identidad. Disponible *[Internet]*:

http://blogs.periodistadigital.com/tecnologia.php/2008/12/19/las-redes-sociales-y-el-openid

[20].Artículos relacionados con el SPAM. Disponible *[Internet]*:

- Ejemplo de cómo protegernos (*javascript*):

  http://javascript.internet.com/page-details/disable-text-selection.html

- Ejemplo de cómo romper la protección: http://www.carlosleopoldo.com/post/copiar-texto-paginas-protegidas/
- Algunas técnicas: http://www.alejandrox.com/2009/01/tecnicas-para-evitar-el-spam/
- Servicio gratuito de CAPCHAS: http://www.desarrollo*web*.com/faq/que-es-captcha.html

[21].Artículos relacionados con el *Phishing*, *SSL* y *EV-SSL*. Disponible *[Internet]*:

- *How does SSL prevent phishing? It doesn*'t: http://voices.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html
- EV-SSL: http://eu.globalsign.com/digital-certificate/extended-validation-ssl/index.htm
- Lucha contra el *phising*: 44 maneras de protegerte: http://www.logadmin.net/2007/01/lucha-contra-el-phising-44-maneras-de.html

- *Paypal FAQ*: https://www.paypal.com/es/cgi-bin/*web*scr?cmd=xpt/Marketing/securitycenter/general/UnderstandPhishing-outside
- *Anti-pishing.org*: http://www.antiphising.org
- *Anti-phising browsers plugin*:
  - http://addins.msn.com/phishingfilter
  - https://addons.mozilla.org/en-US/firefox/addon/2366
  - http://blogs.msdn.com/ie/archive/2005/09/09/463204.aspx
- http://www.microsoft.com/mscorp/safety/technologies/antiphishing/default.mspx

[22].*McAfee Research Anti-Phishing: Best Practices for Institutions and Consumer*s. Disponible *[Internet]*: http://www.mcafee.com

[23].*TOKENS*. Disponible *[Internet]:* http://es.wikipedia.org/wiki/Token_de_seguridad

[24].Observatorio de Evolución de las redes sociales. Disponible *[Internet]:*

http://www.tcanalysis.com/uploads/2008/11/informe_observatorio_redes_sociales.pdf

[25]. C*hild Grooming*. Disponible *[Internet]: http://es.wikipedia.org/wiki/Grooming*

[26].*Ciberbullying.* CiberAcoso España*.* Disponible *[Internet]: http://es.wikipedia.org/wiki/Ciberacoso.*

[27].Artículo acerca de las futuras nuevas tecnologías para proteger a los menores en las redes sociales:

- http://www.vanguardia.com.mx/diario/noticia/tech/tecnologia/acuerda_facebook_proteger_a_sus_clientes_menores_de_edad/163380
- Mecanismos de autenticación intermedios en fase beta en *Twitter*: http://apiwiki.twitter.com/Sign-in-with-Twitter basado en *OAuth*: http://oauth.net/documentation/getting-started
- *Facebook* con FB *Connect*: http://mashable.com/2009/04/18/twitter-facebook-connect/
- Otros mecanismos de autenticación: http://www.aladdin.es/PressReleases/post/Aladdin-eSafe,-el-primero-en-ofrecer-control-para-aplicaciones-*web*-20.aspx
- Artículo acerca de la autenticación robusta: http://www.prensa.com/actualidad/tecnologia/2005/10/27/index.htm

[28].*Cloud Computing*. Información en la nube España. Disponible *[Internet]*: *http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_nube*

[28-a]. *ATP (Advanced Persistent Threat).* Disponible *[Internet]*: http://www.magazcitum.com.mx/?p=1547

[29].*Final Report of ISTTF (Internet Safety Technical Task Force) Enhancing Child Safety & Online Technologies*. Disponible *[Internet]*: http://cyber.law.harvard.edu/research/isttf

[30].Junto al valor de la vida humana y sustancialmente relacionado con la dimensión moral de ésta, nuestra Constitución ha elevado también a valor jurídico fundamental la dignidad de la persona, que, sin perjuicio de los derechos que le son inherentes, se halla íntimamente vinculada con el libre desarrollo de la personalidad (art. 10) y los derechos a la integridad física y moral (art. 15), a la libertad de ideas y creencias (art. 16), al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1). Del sentido de estos preceptos puede deducirse que la dignidad es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás.ò(STC 53/1985 FJ núm. 8).

[31].El derecho a la propia imagen, consagrado en el art. 18. 1 CE junto con los derechos a la intimidad personal y familiar y al honor, contribuye a preservar la dignidad de la persona (art. 10. 1 CE), salvaguardando una esfera de la propia reserva personal, frente a intromisiones de terceros. Sólo adquiere así su pleno sentido cuando se le enmarca en la salvaguarda de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humanaò(STC 99/1994).

[32].El Convenio de Roma de 1950 regula el derecho a la vida privada en su artículo 8 en los siguientes términos:

> Derecho al respeto a la vida privada y familiar
>
> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad

democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Instrumento de Ratificación de 26 de septiembre de 1979.

[33].Informe de la Agencia Española de Protección de Datos 327/2003. Disponible *[Internet]*: https://www.agpd.es/portal*web*/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf

[34].Dictamen sobre el concepto de datos personales. El Grupo de trabajo considera las direcciones IP como datos sobre una persona identificable. En ese sentido ha declarado que «los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva. Disponible *[Internet]*: (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_es.pdf).

[34b].Disponible *[Internet]*: http://www.asegurdat.com/LOPD/sello.htm

[35].Directrices de la OCDE sobre protección de la privacidad y flujos de datos personales, de 23 de septiembre de 1980. Disponible *[Internet]*: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[36].Directrices para la regulación de los archivos de datos personales informatizados, Adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990 de la ONU.

[37].*Asia-Pacific Economic Cooperation Privacy Framework*. Disponible *[Internet]*: http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

[38].Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984 (B.O.E. de 15 de noviembre de 1985).

[39].Resolución (73) 22 relativa a la protección de la vida privada de la personas físicas respecto de los bancos de datos electrónicos en el sector privado, acordada por el Comité de Ministros el 26 de septiembre de 1973.

[40].Resolución (74) 29 relativa a la protección de la vida privada de la personas físicas respecto de los bancos de datos electrónicos en el sector público, adoptada por el Comité de Ministros el 20 de septiembre de 1974.

[41].Disponible *[Internet]*:
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML

[42].Disponible *[Internet]*: http://ec.europa.eu/justicehome/fsj/privacy/workinggroup/index_en.htm

[43].Un ejemplo claro es el caso de la sentencia dictada en el caso de la Sra. *Lindqvist*, acusada de haber infringido la normativa sueca relativa a la protección de datos personales al publicar en su sitio *web* diversos datos de carácter personal sobre varias personas que, como ella, colaboraban voluntariamente con una parroquia de la Iglesia protestante de Suecia. Esta señora, habiendo aprendido rudimentos de informática y diseño *web*, mantenía una página de información parroquial en la que llegó a informar sobre el estado de salud de un miembro de la comunidad. Respondiendo a las cuestiones planteadas el TJCE identificó la presencia de un tratamiento de datos de carácter personal sujeto a la Directiva.

[44].Disponible *[Internet]*: https://www.agpd.es/portal*web*AGPD/index-ides-idphp.php

[45].Disponible *[Internet]*:
http://eurex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:ES:PDF

[46].Disponible *[Internet]*:
https://www.agpd.es/portal*web*/canaldocumentacion/internacional/common/pdf/WP_148_Dictamen_Buscadores_es.pdf

[47].Disponible *[Internet]*:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf

[48].*web Bug. Baliza web España.* Disponible *[Internet]*:

http://es.wikipedia.org/wiki/*web*_bug

[49].El artículo ñRecomendaciones para la creación y uso de contraseñas segurasò del Observatorio de la Seguridad de la Información de INTECO ofrece información relevante para un uso adecuado de contraseñas.

[50].Art.2 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[51].Art.1 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[52].Disponible *[Internet]*: www.fiscal.es/fiscal/public

[53].Disponible *[Internet]*:

http://www.revistagestiondocumental.com/2010/10/05/asimelec-presenta-el-informe-2010-contenidos-digitales/

[54].Promusicae. Productores de música España. Disponible *[Internet]*: http://es.wikipedia.org/wiki/Productores_de_M%C3%BAsica_de_Espa%C3%B1a

[55]. Disponible *[Internet]*: http://www.elmundo.es/elmundo/2009/11/05/navegante/1257414681.html

[56]. Secretaría de Estado de Cultura. Disponible *[Internet]*: http://www.mcu.es/

[57].Memoria AEPD 2007, recomendación normativa 2ª. Disponible *[Internet]*: https://www.agpd.es/portal*web*AGPD/canaldocumentacion/publicaciones/common/pdfs/memoria_AEPD_2007.pdf

[58].Concepto dispuesto por el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

[59].Disponible *[Internet]*: http://www.elmundo.es/elmundo/2012/01/25/navegante/1327485351.html

[60].Disponible [*Internet]*: http://www.elmundo.es/elmundo/2010/06/06/navegante/1275818715.html

[61].Disponible *[Internet]*: http://www.elmundo.es/elmundo/2011/03/17/navegante/1300359389.html

[62].Según la definición dispuesta en la Disposición Adicional Primera de la Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico, se trata de toda ***ñ****persona física o jurídica que proporciona un servicio de la sociedad de la información****ò***

Referencias Figuras:

[REF_FIG0]. Representación gráfica de una Red Social. Disponible *[Internet]*: http://www.adaspirant.com/articulos.php

[REF_FIG1]. Usuario de las principales Redes Sociales. Disponible *[Internet]*: http://www.concepto05.com/2012/01/estadisitica-usuarios-de-redes-sociales-en-espana-2012/

[REF_FIG2]. Notifica de espionaje en *facebook*. Disponible *[Internet]*:

http://www.publico.es/ciencias/174793/espionaje-entre-trabajadores-a-traves-de-facebook

[REF_FIG3]. Ventana falsa que replica la el sistema de conexión a *facebook*. Disponible *[Internet]*: http://www.elmundo.es/elmundo/2011/03/17/navegante/1300359389.html

[REG_FIG5]. Mcafee Anti-Phishing. Disponible *[Internet]*:

http://www.distrodocs.com/17194-anti-phishing-best-practices-for-institutions-consumer

[REG_FIG7]. Redes Sociales integradas en dispositivos. Disponible *[Internet]*:

http://blog.3dcart.com/tag/facebook-connect/